Universidad de Cuenca

Facultad de Ingeniería

Escuela de Electrónica y Telecomunicaciones

Análisis digital forense de los sensores de un teléfono inteligente para la detección y recreación de actividad motriz inusual en una localización determinada

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Director :

Ing. Karina Pamela Campos Argudo, Mgst

Autores :

David Antonio Espinoza Farfán

Juan Martín Yánez Rodas

Cuenca - Ecuador

2016

Resumen

El objetivo de la presente investigación es desarrollar una nueva metodología para la detección y recreación de la actividad motriz inusual de una posible víctima en una localización determinada. Este trabajo se enmarca dentro del campo del análisis digital forense, rama de la criminalística que se encarga de la obtención de potencial evidencia digital de dispositivos electrónicos con fines penales mediante la aplicación de un conjunto de técnicas y procedimientos adecuados.

Este trabajo tiene como base la utilización de información proveniente de un teléfono inteligente, por lo que en primera instancia se desarrolla una aplicación para el sistema operativo Android que tiene como función la extracción y registro de mediciones de ciertos sensores del dispositivo. Una vez almacenada la información se procede con el procesamiento y análisis de los datos en *Matrix Laboratory* (MATLAB), a partir de lo cual se logra la identificación de movimientos bruscos sin importar el tipo de actividad realizada por la víctima en el momento del siniestro. Finalmente, se desarrolla una aplicación de escritorio en la misma plataforma que consta de una interfaz gráfica en la que se presenta la reconstrucción digitalizada en tres dimensiones de la trayectoria que siguió la víctima, así como la geolocalización del sitio exacto en el que ocurrió el siniestro. Dentro de la aplicación de escritorio también se presenta otro tipo de información relevante para la investigación forense como es la aceleración resultante antes y después de la ocurrencia de actividad inusual, fecha y hora, número de pasos dados por la víctima y distancia total recorrida.

Palabras claves: análisis digital forense, evidencia digital, sensores, acelerómetro, aceleración resultante, detección, actividad inusual, recreación gráfica.

Abstract

The objective of this research is to develop a new methodology in order to detect and recreate unusual motor activity from a possible victim in a determined location. This work is framed within the field of digital forensic analysis, branch of criminology which is in charge of obtaining potential digital evidence from electronic devices with criminal purposes by applying a set of adequate techniques and procedures.

This work has as its base the use of information obtained from a smartphone, so in first instance an application for the Android operative system is developed with the purpose of extracting and registering measurements from some sensors of the device. Once the information is stored it is processed and analyzed in MATLAB, from which the identification of abrupt movements is achieved regardless of the type of activity performed by the victim at the time of the incident. Finally, a desktop application is developed in the same platform, it contains a graphical interface in which is presented the digitalized reconstruction in three dimensions of the trajectory followed by the victim, as well as the geographic location of the exact site where the incident occurred. In the desktop application is also presented other information relevant to the forensic research like the resultant acceleration before and after the occurrence of unusual activity, the date and hour, number of steps taken by the victim and the total distance of displacement.

Keywords: digital forensics analysis, digital evidence, sensors, accelerometer, resultant acceleration, detection, unusual activity, graphic recreation.

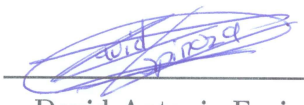
Yo, David Antonio Espinoza Farfán, autor de la tesis "Análisis digital forense de los sensores de un teléfono inteligente para la detección y recreación de actividad motriz inusual en una localización determinada", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 17 de marzo del 2016

David Antonio Espinoza Farfán
0104426879

Yo, David Antonio Espinoza Farfán, autor de la tesis "Análisis digital forense de los sensores de un teléfono inteligente para la detección y recreación de actividad motriz inusual en una localización determinada", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de ingeniero en Electrónica y Telecomunicaciones. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

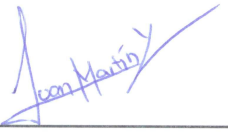
Cuenca, 17 de marzo del 2016



David Antonio Espinoza Farfán
0104426879

Yo, Juan Martín Yánez Rodas, autor de la tesis "Análisis digital forense de los sensores de un teléfono inteligente para la detección y recreación de actividad motriz inusual en una localización determinada", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 17 de marzo del 2016



Juan Martín Yánez Rodas
0104720842

Yo, Juan Martín Yánez Rodas, autor de la tesis "Análisis digital forense de los sensores de un teléfono inteligente para la detección y recreación de actividad motriz inusual en una localización determinada", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de ingeniero en Electrónica y Telecomunicaciones. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 17 de marzo del 2016

Juan Martín Yánez Rodas
0104720842

Dedicatoria

Dedico esta tesis a mis padres Marco Antonio y Marcia Eulalia quienes en todo momento me brindaron su apoyo incondicional, guiándome y dándome las pautas necesarias para poder concluir esta etapa de mi vida, a mi hermano Esteban y a mis hermanas Verónica y Jessica por siempre estar presentes en los momentos de dificultad y ser pilares fundamentales en mi vida.

David Antonio

Dedico esta tesis a mi padre, Joaquín, por ser ese ejemplo de lucha que me inspira cada día a superar cualquier adversidad sin importar lo difícil que parezca la situación, por su apoyo y por su amor incondicional hacia sus hijos. A mis hermanos Francisco y Joaquina, por darme las fuerzas necesarias para terminar mi carrera universitaria y por ser el pilar fundamental de mi existencia. A Yadira, por ser la mujer que me complementa, mi fuente de alegría y felicidad, por su ayuda total en el cumplimiento de mis metas personales.

Juan Martín

Agradecimientos

Agradecemos principalmente a la Ing. Karina Campos por su acertada labor como guía a lo largo del desarrollo de la presente investigación, por su tiempo, esfuerzo y dedicación. También queremos agradecer a los profesores de la facultad en general por su ayuda desinteresada ante cualquier duda o aclaración referente a la realización de esta tesis.

David Antonio, Juan Martín

Índice general

Índice de figuras

Índice de tablas

Abreviaciones y Acrónimos

ACPO *Association of Chief Police Officers*. 26, 27
AMPS *Advanced Mobile Phone System*. 14, 15
API Interfaz de Programación de Aplicaciones. 19

BES *BlackBerry Enterprise Server*. 22
BIS *BlackBerry Internet Service*. 22

DFRWS *Digital Forensic Research Workshop*. 7
DVM Máquina Virtual Dalvik. 19

FAT *File Allocation Table*. 26
FTT *Fast Fourier Transform*. 31

GPS Sistema de Posicionamiento Global. 5, 25, 29, 35, 37, 42, 43, 59, 84, 85
GSM *Global System for Mobile Communications*. 16

HSPA *High Speed Packet Access*. 16

IDC *International Data Corporation*. 3
IDE *Integrated Development Environment*. 35, 47, 85
IP *Internet Protocol*. 17
IPTV Televisión por Internet. 17
IS Estándar Interno. 16
ISO/IEC *International Organization for Standardization/International Electrotechnical Commission*. 28

LAN *Local Area Network*. 16

MATLAB *Matrix Laboratory*. 5, 38, 47–50, 69, 76, 85
MEMS *Micro Electro Mechanical System*. 24
MIDP *Mobile Information Device profile*. 21

MTi *Motion Trackers*. 30

NAMTS *Nippon Advanced Mobile Telephone Service*. 15
NAS *Network Attached Storage*. 12
NCC *Zero-Normalized Cross Correlation*. 31
NMTS *Nordic Advanced Mobile System*. 15
NTT *Nippon Telegraph And Telephone Corp*. 14

OS-móvil Sistema Operativo Móvil. 18

PDA Asistente Personal Digital. 18
PWB *Printed Wiring Board*. 17

RIM *Research in Motion*. 21

SAN *Storage Area Network*. 12
SS Sitio del Suceso. 2, 4, 5, 10–12, 35–38, 73, 77, 85
SVM *Support Vector Machine*. 31

TACS *Total Access Communications System*. 15

UID Identificador de Usuario Unix. 19
UMTS *Universal Mobile Telecommunications System*. 16

WAP Protocolo de Aplicaciones Inalámbricas. 17, 21

Capítulo 1

Introducción

1.1. Estudio del problema

Actualmente en el Ecuador, y según el último Código Orgánico Integral Penal publicado en el mes de febrero del año 2014 [7], es posible utilizar como medio de prueba todo contenido digital proveniente de dispositivos electrónicos mediante la utilización de técnicas digitales forenses adecuadas y aprobadas por el mismo código. Debido a la reciente inclusión de este tipo de evidencia en procesos judiciales no solamente en nuestro país sino a nivel mundial, existen pocos peritos sobre el tema, de hecho, según [8], el porcentaje de agentes de la ley en Estados Unidos que cuentan con una formación especializada en investigación informática o digital es solo del 20 %. De igual forma existen escasas técnicas de obtención y recuperación de contenido digital que pueda llegar a constituirse en un argumento factible para la resolución de un caso, por lo que resulta imprescindible la investigación académica referente a este campo con el fin de contribuir con metodologías o aplicaciones que faciliten y agilicen dichos procesos.

El análisis o peritaje digital constituye una de las ramas de más reciente auge dentro del ámbito forense, sin embargo, es una de las disciplinas con mayor potencial ya que mediante este tipo de investigación es posible extraer información de un siniestro que de otra forma sería muy difícil o imposible. Hoy en día, distintos dispositivos electrónicos, en especial los teléfonos inteligentes, constituyen una fuente valedera de evidencia, que puede ser utilizada en un juicio si se realiza de manera correcta el peritaje respectivo con el fin de obtener e interpretar la información que estos son capaces de proporcionar.

En años recientes, un sin número de casos han podido ser resueltos gracias a pericias bien ejecutadas relacionadas al contenido digital encontrado en diversas formas y en diversos dispositivos electrónicos. Uno de los casos de mayor renombre es el del

autodenominado asesino BTK en Estados Unidos, quien luego de un largo historial de asesinatos pudo ser identificado y rastreado gracias a la información contenida en los metadatos de un archivo de texto que grabó en un disquete y envió a la policía. Otro de los casos relacionados al análisis digital forense, es el del secuestrador Scott Tyree, quien mantenía cautiva a una joven de apenas 13 años, luego de enviar un mensaje instantaneo con una foto de la víctima a través de un servicio web a otro internauta, pudo ser rastreado mediante su alias *"masterforteenslavegirls"* que lo vinculaba con su dirección IP, y por lo tanto, su ubicación física [9]. Varios procesos judiciales como los anteriores han llegado a su fin gracias a la aplicación de técnicas digitales forenses adecuadas, aunque cabe recalcar, que gran parte de la potencial evidencia se pierde o se invalida debido a procedimientos defectuosos de valoración, recuperación o presentación de pruebas digitales, de ahí la importancia de la presente investigación, que tiene como finalidad colaborar en la resolución de distintos casos judiciales.

Dentro del análisis digital forense la mayoría de metodologías tiene como objetivo adquirir evidencias relacionadas con la interacción de la víctima y sus dispositivos electrónicos dentro del campo enteramente digital, es decir, se enfocan principalmente en la extracción de archivos, registros, historiales, etc. Que pudieran relacionarse con las circunstancias del siniestro.

En esta investigación se propone una nueva metodología, que se enfoca en la extracción de la información referente a la actividad motriz de la víctima, es decir, se basa en el mismo principio básico de anteriores técnicas de obtener información digital de los dispositivos pero de fuentes distintas como son los sensores con los que cuentan los teléfonos inteligentes. Varios de estos sensores pueden entregar información referente al movimiento de la víctima en cualquier instante, y de hecho se han utilizado para la creación de aplicaciones de ocio o relacionadas con el ejercicio físico, pero nunca antes se habían utilizado estos recursos para la detección de actividad motriz inusual dentro del SS.

La presente investigación no contempla únicamente fines académicos sino también sociales, ya que de concretarse una herramienta que permita la identificación de actividad motriz inusual de una víctima, así como la recreación de la trayectoria que ésta siguió en el momento del siniestro, no solamente sería un gran avance para el campo forense local y mundial dado que aportaría con evidencia de relevancia para la resolución de un juicio, sino que disminuiría el nivel de inseguridad que sufren varios sectores de la sociedad.

1.2. Justificación

En la actualidad debido a la generalización tecnológica que ha tenido la sociedad en los últimos años, existe una gran aumento en la demanda de teléfonos inteligentes por año (véase Figura 1.1), las ventas mundiales de este tipo de dispositivos fueron de 968 millones de unidades en el 2013, un aumento del 42,3 % en comparación con el 2012. La *International Data Corporation* (IDC) predice que este número habrá aumentado a 1,2 billones de unidades en 2014 y 1,7 billones de unidades en 2018 [10]. Como se observa, existe una gran cantidad de dispositivos vendidos por lo que un importante porcentaje de la población cuenta con un teléfono inteligente o un dispositivo móvil de características similares en todo momento. De hecho, en 2011 la penetración de teléfonos inteligentes mundial per cápita fue de 9,6 %. En 2017, se prevé que la penetración mundial de teléfonos inteligentes per cápita puede llegar a 34,2 % [11]. Dichos dispositivos se han convertido en una herramienta importante en el diario vivir de las personas, haciendo de estos, una potencial fuente de información para la investigación forense debido a la variedad de sensores con los que cuentan y los tipos de datos que estos son capaces de recopilar.

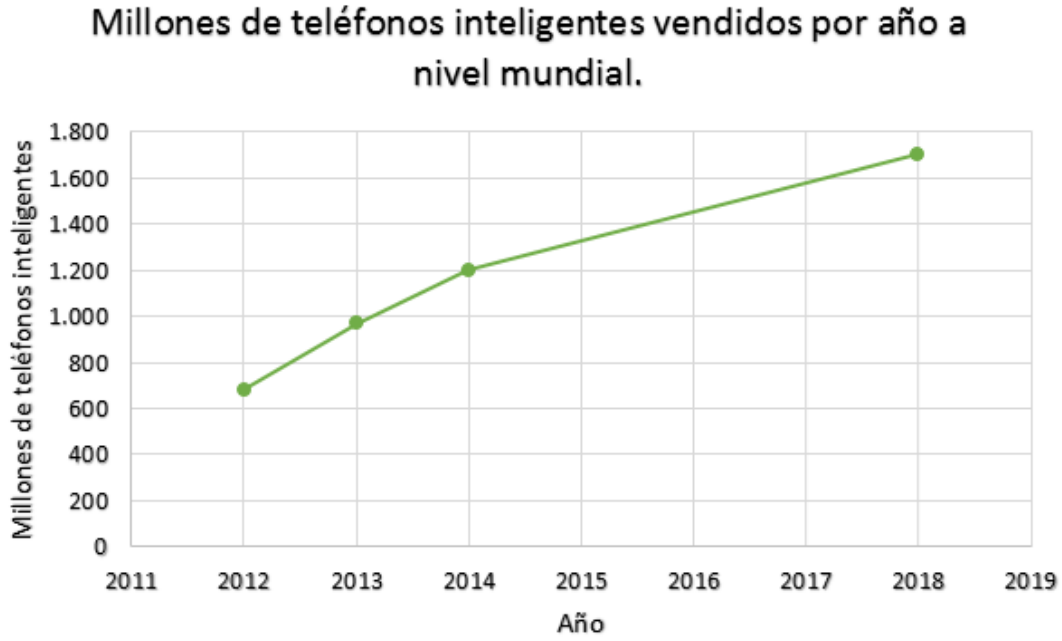


Figura 1.1: Millones de teléfonos inteligentes vendidos por año a nivel mundial.

Una de las consecuencias más relevantes de estos hechos, es el posible monitoreo que podría realizarse de la actividad que realiza una persona, no solo aquella llevada a cabo de forma digital o en la web, sino también al tipo de actividad relacionada con los movimientos e interacciones que tiene una persona en todo momento, o también llamada actividad motriz. Por lo que potencialmente, la mayoría de la población, no solo cuenta con un asistente tecnológico personal, sino con un testigo silencioso y vigilante a la mano o en su bolsillo en todo momento.

Con esta premisa, se introduce el concepto de la identificación de la actividad de un individuo a partir de los datos obtenidos por los sensores de movimiento de un teléfono inteligente, lo cual puede ser de gran ayuda al momento de realizar un análisis digital forense, ya que permitiría identificar movimientos bruscos realizados por una víctima en el SS y además, recrear con gran exactitud su trayectoria de movimiento.

1.3. Objetivos

1.3.1. Objetivo general

Detectar y recrear actividades relevantes para el análisis digital forense, con la ayuda de los sensores de un teléfono inteligente, en el sitio del suceso.

1.3.2. Objetivos específicos

- Realizar una aplicación Android que permita registrar mediciones de los sensores del teléfono inteligente.
- Efectuar un procesamiento en tiempo real con el fin de activar y almacenar datos del GPS según medidas abruptas del acelerómetro.
- Optimizar el sistema de almacenamiento de los datos obtenidos por los sensores del teléfono móvil, con el fin de utilizar la menor cantidad de memoria interna como sea posible.
- Desarrollar un algoritmo capaz de identificar actividades inusuales a partir de los datos obtenidos por la aplicación.
- Realizar una reconstrucción gráfica de los hechos mediante una aplicación de escritorio.

1.4. Alcance

Como eje principal de la presente investigación se tiene la detección en tiempo real de actividad motriz inusual o abrupta realizada por una persona mediante los datos entregados por el acelerómetro de un teléfono inteligente. Se pretende además, establecer la localización exacta del lugar de los hechos o del también llamado SS con la ayuda del Sistema de Posicionamiento Global (GPS), solo cuando se ha dado la detección mencionada anteriormente, esto con el fin de evitar una violación a la privacidad de la víctima mediante el almacenamiento continuo de su ubicación. Finalmente, se pretende extraer datos referentes a la orientación, desplazamiento horizontal y vertical del dispositivo. Los datos de la orientación son proporcionados por la combinación de dos sensores, el giroscopio y el magnetómetro, los datos del desplazamiento horizontal son proporcionados por el contador de pasos y los datos del desplazamiento vertical por el barómetro, esto con el objetivo de llevar a cabo una recreación de la trayectoria realizada por la víctima en caso de que ésta sufra algún incidente. Todos estos datos proporcionados por los sensores del teléfono inteligente serán extraídos y almacenados mediante una aplicación Android creada desde cero para esta investigación en específico. Se optimizará el almacenamiento en el dispositivo buscando el menor consumo posible de memoria, ya que la aplicación guardará los datos de los sensores continuamente en archivos de texto por el transcurso de una hora, al finalizar este tiempo la aplicación será capaz de comprobar si existió o no algún tipo de actividad inusual o abrupta, al existir este tipo de actividad inusual los datos permanecerán almacenados en los archivos de texto con un nombre específico, en el caso de no existir esta actividad inusual los archivos de texto serán eliminados automáticamente para luego continuar con el almacenamiento de los datos siguientes.

Posterior a la recopilación de la información, se llevará a cabo un procesamiento de la información entregada por la aplicación mediante el uso de distintos procedimientos matemáticos y gráficas a partir de la herramienta de software matemático MATLAB, con el fin de analizar, comprender y discernir entre los datos valederos y los no valederos para así identificar actividad inusual realizada por la víctima de una manera mucho más precisa y detallada.

Por último, y luego de haber realizado el procesamiento de la información, se realizará el diseño y la programación de una interfaz gráfica en el propio MATLAB que permita la recreación en tres dimensiones de la trayectoria de la víctima en los puntos de interés a lo largo del tiempo.

Ya que el presente proyecto esta dedicado específicamente para el análisis digital

forense, los usuarios a los que esta dirigido son aquellos que intervienen directamente en el siniestro, como pueden ser la fiscalía, el departamento de policía, peritos en el tema o incluso la víctima, por lo que la interfaz pretende brindar un ambiente amigable mediante el cual se pueda navegar a través del tiempo y a la vez reconstruir los hechos del siniestro.

Capítulo 2

Marco teórico y estado del arte

2.1. Análisis digital forense

El análisis digital forense es un campo aplicado de las ciencias forenses que tiene como objetivo el descubrimiento, identificación y análisis de información representada por medio de formatos digitales. Dicha rama forense busca que esta información pueda ser utilizada en entornos legales como pruebas o evidencias fehacientes sobre un crimen cometido [12].

Según el *Digital Forensic Research Workshop* (DFRWS), una organización de voluntarios sin fines de lucro dedicados al intercambio de ideas y conocimientos sobre el análisis digital forense, en su reporte técnico "*A road map for digital forensic research*", resultado de una convención del cuál fueron participes más de 50 investigadores universitarios, examinadores forenses de computadoras y analistas relacionados al tema, definen a la ciencia digital forense como [13]:

> El uso de métodos probados y derivados científicamente, para la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital proveniente de fuentes digitales con el propósito de facilitar y promover la reconstrucción de hechos de carácter criminal, o ayudar a prevenir acciones no autorizadas que pueden ser perjudiciales para operaciones planificadas.

El auge de esta rama pericial en los últimos años se debe, principalmente, al surgimiento de una nueva clase de crímenes relacionados con dispositivos que utilizan tecnologías electrónicas digitales y con aquellos delitos que se perpetran en Internet.

A pesar de que la mayoría de la evolución tecnológica se ha dado en busca de ciertos aspectos como el menor consumo de energía, mayor capacidad computacional

y una mejor eficiencia, el surgimiento de productos orientados al consumidor como los teléfonos móviles, reproductores multimedia y dispositivos personales similares, ha dado como resultado un cierto tipo de convergencia entre la tecnología y la moda, llevando así a la humanidad a una generalización tecnológica digital. En muchos de los casos, especialmente entre los miembros más jóvenes de la sociedad, resulta una necesidad primordial el poseer alguno de estos dispositivos con el fin de encajar dentro de un grupo social en particular. Este comportamiento social está implícito en los seres humanos y ocurre en diferentes aspectos como en los gustos musicales o en la afición por algún equipo de fútbol [14]. Por lo que el surgimiento del análisis digital forense como una ciencia queda totalmente justificado al ser una parte imprescindible de la investigación pericial en la actualidad, ya que evidencia que puede ser de ayuda para la resolución de un caso, solo puede ser extraída de dispositivos como los mencionados anteriormente.

Además, gracias al acceso extendido de la población a este tipo de dispositivos y tecnología en los últimos años, la incidencia de crímenes cibernéticos es cada vez mayor y por lo tanto, en todo el mundo, agencias de justicia criminal especializadas están siendo conformadas para la investigación de delitos cometidos parcial o enteramente en Internet u otro tipo de medio electrónico [15].

A continuación se detalla la metodología para el manejo de evidencia digital, la cual consta de cuatro procesos fundamentales que son la identificación, recolección, adquisición y preservación de potencial evidencia [16], no sin antes definir claramente el concepto de evidencia digital así como sus categorías.

2.1.1. Evidencia digital

Se puede definir a la evidencia digital como toda información o datos, transmitidos o almacenados en formato binario que pueden ser utilizados como pruebas legales [16]. Existen diversas y variadas fuentes de evidencia digital, como los sistemas computarizados entre los cuales constan unidades de almacenamiento, teclados, computadoras portátiles o *laptops*, computadoras de escritorio, servidores entre otros. Estos sistemas, con la constante expansión de su capacidad de almacenamiento, pueden constituirse en una gran fuente de evidencia, un simple archivo puede contener información incriminatoria en su contenido o en sus propiedades como su fecha de creación, quien lo creó o si fue creado en otra computadora. También están los sistemas de comunicación, ejemplos de estos son los sistemas telefónicos tradicionales, sistemas de telecomunicación inalámbricos, Internet, y redes en general, todos estos pueden ser fuentes de evidencia

digital. La forma en la que se obtiene evidencia de este tipo de sistemas es analizando los registros o logs de servidores o *routers* a partir de los cuales, un mensaje, *email* o información en general fue enviada o recibida. Algunos sistemas de comunicación pueden ser incluso configurados para capturar todo el contenido digital o tráfico de datos que pasa por estos. Por último están los sistemas informáticos integrados como los teléfonos inteligentes, tabletas, sistemas de navegación, cámaras fotográficas digitales, reproductores multimedia, etc. La evidencia que se obtiene de estos dispositivos depende el tipo de datos que pueden otorgar o almacenar, por ejemplo en los teléfonos inteligentes es posible obtener fotografías, videos, registros de comunicaciones, y hasta información personal relacionada con la ubicación geográfica del propietario del dispositivo o su actividad motriz en cualquier instante [17].

Todos los sistemas y dispositivos mencionados anteriormente pueden diferenciarse en dos grandes grupos que son los sistemas cerrados o sistemas abiertos.

Un sistema cerrado, desde el punto de vista de un investigador forense, es aquel sistema que nunca ha estado conectado a Internet. Es decir, constituye un dispositivo que ha existido como una entidad aislada dentro de un ambiente conocido y controlado. Todos los dispositivos a los que alguna vez pudo haber sido conectado, han sido también sistemas cerrados, creando así redes cerradas, otra forma de sistemas cerrados. Por lo tanto, se puede decir que un sistema cerrado, consiste o está conformado por sistemas más pequeños, los cuales satisfacen la definición de un sistema cerrado [14].

En contraste, un sistema abierto, es cualquier sistema que en algún momento de su vida útil tuvo alguna clase de conexión a Internet. Esta conexión puede haber sido directa, como por ejemplo una conexión a una red inalámbrica en una universidad, o indirecta, como por ejemplo mediante el uso de un dispositivo de almacenamiento que previamente fue conectado a un sistema con acceso a Internet. No importa la forma de conexión, cualquier asociación con Internet convierte a un sistema cerrado en uno abierto [14].

Para el análisis digital forense, esta clasificación es de gran importancia. Se considera el siguiente ejemplo sobre una escena del crimen convencional. Se ha producido la muerte de un individuo en circunstancias no del todo claras, y que su cuerpo ha sido descubierto. Si el cuerpo fue encontrado en una habitación que tenía todas sus ventanas y puertas cerradas desde el interior, se puede asumir, con un razonable grado de confianza, que cualquier cosa que le haya ocurrido a la víctima debió haber pasado dentro de esa habitación, y que la causa de muerte y cualquier evidencia relacionada con el siniestro puede estar presente aún. Ningún objeto fue extraído o introducido de la habitación. Al contrario, si el cuerpo fue encontrado en una calle muy transitada, se

puede afirmar que la evidencia esta contaminada por el cambiante ambiente que rodea al cuerpo. Fibras, escombros, y hasta material biológico están siendo levantados por el viento hacia el cuerpo o sacudidas de la ropa de la víctima. En efecto, un sistema digital cerrado, tiene su analogía con la habitación cerrada. No importa que tan grande es la red de sistemas cerrados, siempre es posible determinar su perímetro e identificar todos y cada uno de los dispositivos en la misma. Sin embargo, con un sistema abierto, ocurre todo lo contrario, varios sistemas se unen o dejan Internet cada segundo de cada día. Nuevos programas son creados, los sistemas cambian de estado, los usuarios crean diferentes tipos de tráfico o transferencia de datos. El hecho de que resulta imposible registrar con precisión el estado completo de Internet en cualquier momento, introduce nuevas oportunidades de contaminación para la escena del crimen virtual. Por lo que, con sistemas abiertos, siempre se tendrá cierto grado de incertidumbre con respecto a la comprensión de la escena del crimen virtual [14].

Como regla general, los sistemas abiertos, constituyen mejores fuentes de información sobre las personas, sus actividades, hábitos e intereses. Esto se debe a que dichos sistemas tienen acceso a la red más grande del mundo como lo es Internet, en donde, la comunicación es el propósito principal y por ende, cualquier sistema conectado, típicamente contendrá cantidades masivas de datos que no son más que la representación de interacciones con otros dispositivos en la red, y de los cuales se puede extraer información relevante para la resolución de un caso. Por otro lado los sistemas cerrados, tienen poco valor como fuentes de evidencia ya que son usados por las personas para unas pocas y contadas tareas, y no tienen contacto con el mundo exterior hablando en términos digitales [14].

Finalmente se puede decir que en la mayoría de jurisdicciones y organizaciones, la evidencia digital esta gobernada por tres principios fundamentales que son la relevancia, la fiabilidad y la suficiencia. La evidencia digital es relevante cuando se utiliza con el fin de aprobar o desaprobar una hipótesis dentro del siniestro que es motivo de la investigación, y no solo se refiere a la evidencia digital que se pretende sea admisible en el juicio. Mientras que la evidencia digital cumple con el principio de fiabilidad cuando ésta ha sido manipulada de forma correcta por los investigadores y por lo tanto no ha sufrido ningún tipo de alteración. Y finalmente, el principio de suficiencia se refiere al hecho de que se debe recolectar suficiente evidencia potencial que permita llevar a cabo una adecuada examinación o investigación de los hechos que se llevaron a cabo en el SS [16].

2.1.2. Metodología para el manejo de evidencia digital

Desde los inicios del análisis digital forense, ha existido la necesidad de definir una metodología estandarizada para el manejo de potencial evidencia digital vinculada con los procesos investigativos realizados en el SS por entidades o personas a los que les compete dicha tarea, esto con el fin de que se constituyan en evidencias o pruebas valederas que puedan ser usadas en instancias legales para la resolución de un hecho delictivo.

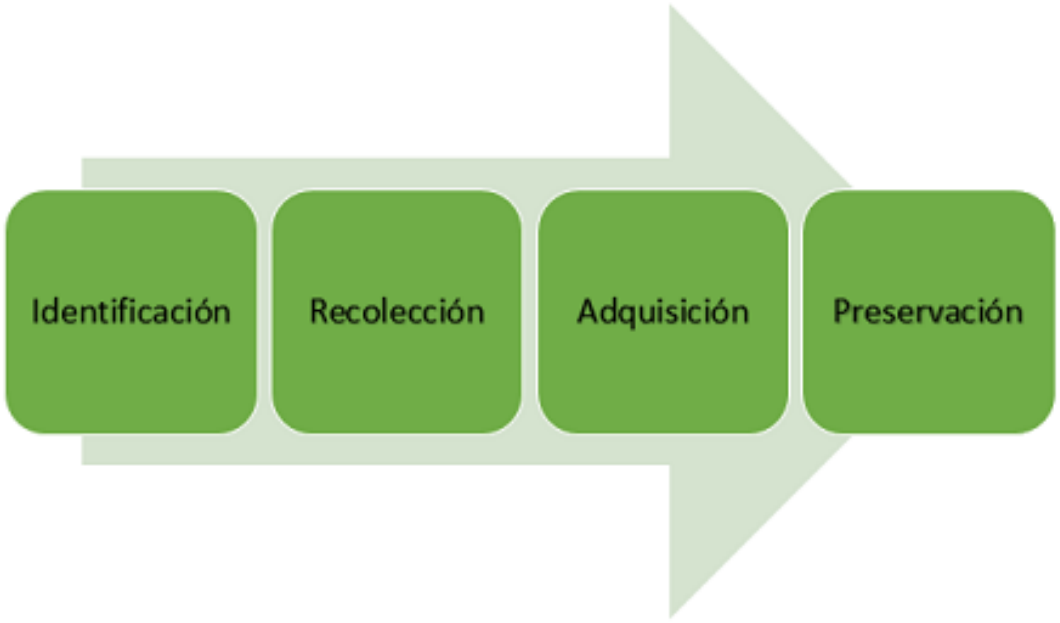


Figura 2.1: Procesos de la metodología para el manejo de evidencia digital.

2.1.2.1. Identificación

La evidencia digital puede presentarse de forma física o lógica. La representación física incluye los dispositivos tangibles de los cuales es posible extraer información, mientras que la representación lógica se refiere a la representación virtual de la información contenida dentro de un dispositivo [16].

El proceso de identificación consiste en la búsqueda, reconocimiento y documentación de potencial evidencia digital. En el proceso de identificación los investigadores deben detectar medios de almacenamiento y dispositivos de procesamiento digital que pudiesen contener potencial evidencia que resulte relevante para el incidente. Dentro de este proceso también se debe incluir cierto grado de prioridad con el objetivo de re-

copilar evidencia con el mayor grado de volatilidad en primera instancia. La volatilidad de los datos es un elemento clave de los mismos, y debe ser identificada apropiadamente para así garantizar un adecuado proceso de recolección y adquisición que minimice el daño o alteración de las pruebas obteniendo así la mejor evidencia. Los peritos en evidencia digital deben estar conscientes de que no todos los medios de almacenamiento digital pueden ser fácilmente identificados y localizados, por ejemplo actualmente existe el almacenamiento y procesamiento de información en la nube, el *Network Attached Storage* (NAS) y también el *Storage Area Network* (SAN) los cuales agregan un componente virtual al proceso de identificación. Finalmente se recomienda que los investigadores lleven a cabo una búsqueda sistemática y cuidadosa de elementos que puedan contener potencial evidencia ya que muchas veces estos son pasados por alto debido a su pequeño tamaño, o debido a que se encuentran encubiertos o embozados junto a otros materiales o dispositivos irrelevantes [16].

2.1.2.2. Recolección

La recolección, es el proceso de manejo de evidencia digital, en el cual los dispositivos considerados como potenciales fuentes de evidencia, son retirados de su ubicación original y trasladados hacia un laboratorio u otro ambiente controlado para la posterior adquisición y análisis de datos. Dichos dispositivos pudiesen encontrase en dos estados, el primero es cuando el sistema se encuentra aún conectado a su fuente de alimentación, y el segundo es cuando el sistema se encuentra desconectado de la fuente de alimentación. Diferentes técnicas y herramientas son necesarias para realizar la recolección de acuerdo al estado del dispositivo. Dentro de este proceso también se incluyen las tareas de documentación de todo el proceso de recolección y el embalaje de los dispositivos identificados previo a su transportación. Es importante que las personas encargadas del SS recopilen cualquier material que pudiera relacionarse con las potenciales fuentes de evidencia digital, como por ejemplo papeles con contraseñas escritas, adaptadores o conectores para la alimentación de energía. Se puede perder o dañar a la potencial evidencia digital si no se aplica un adecuado cuidado de la misma al momento de recolectarla, es por esto que los investigadores deben adoptar el mejor método posible para la recolección basados en la situación, el costo y el tiempo, y documentar el por que de su decisión de haber optado por un método en específico [16].

2.1.2.3. Adquisición

El proceso de adquisición implica la realización de una copia de la evidencia digital, ejemplos de esto son la realización de copias de discos duros en su totalidad o incluso la virtualización completa o creación de la imagen forense de un teléfono inteligente. De igual forma que en procesos anteriores todos los métodos y actividades realizadas deben contar con su respectiva documentación, así como con su debida justificación del por que de la utilización de un método en específico para obtener la copia digital de un dispositivo. Además los métodos y actividades deben ser, como prácticamente sea posible, reproducibles y verificables. Los especialistas en evidencia digital encargados deben realizar la adquisición en la forma menos intrusiva posible con el fin de evitar la alteración de la evidencia, aunque pueden existir procesos de adquisición en los que la alteración de la evidencia es inevitable. Tanto la fuente original como la copia de evidencia digital deben ser verificadas mediante una función de verificación aprobada y aceptada por las entidades de justicia o individuos que harán uso de ésta con los fines que estos consideren adecuados, el original y la copia de la evidencia digital deben producir la misma salida una vez que se aplica la función de verificación a los mismos. Finalmente habrá instancias en las que no será posible la creación de una copia digital de la evidencia como cuando ésta es demasiado larga, hablando en términos de espacio computacional; en estos casos queda a responsabilidad de los peritos desempeñar una adquisición lógica de la evidencia dirigida a recuperar directorios, locaciones y formatos específicos de datos que pudiesen ser relevantes para la investigación [16].

2.1.2.4. Preservación

La potencial evidencia digital debe ser preservada correctamente para asegurar su uso en cualquier momento de la investigación, e incluso en instancias posteriores. Es importante proteger la integridad de la evidencia. El proceso de preservación implica salvaguardar, tanto la evidencia como los dispositivos digitales que la contienen, de la manipulación indebida o innecesaria que pudiese dañar los datos que constituyen la evidencia. Este proceso debe iniciarse y mantenerse a lo largo del proceso completo de manejo de la evidencia digital, es decir desde la identificación hasta la adquisición. En el mejor de los escenarios, no debería existir alteración alguna de la información en sí y de los metadatos asociados a la misma. Los especialistas en evidencia digital o peritos deben ser capaces de demostrar que la evidencia no ha sido modificada desde que fue recolectada o adquirida, o de proveer las razones y acciones documentadas si es que se hicieron cambios inevitables en la evidencia. Finalmente, en algunos casos, la

confidencialidad de la potencial evidencia digital es un requisito imprescindible, ya sea por razones legales o morales, por lo que dicha evidencia debe ser preservada de forma que se garantice la confidencialidad de los datos o información [16].

2.2. Dispositivos móviles celulares

2.2.1. Dispositivos celulares

Un teléfono celular es un dispositivo *full-duplex*. Eso significa que utiliza una frecuencia para hablar y otra frecuencia separada para escuchar. Las dos personas en la llamada pueden hablar al mismo tiempo. Dividir una ciudad en pequeñas celdas permite una amplia reutilización de frecuencias a través, por lo que millones de personas pueden usar teléfonos celulares al mismo tiempo. Los teléfonos celulares operan dentro de celdas, y pueden cambiar de celdas a medida que se mueven dentro de la zona de cobertura. Una persona que usa un teléfono celular puede desplazarse cientos de kilómetros y mantener una conversación todo el tiempo debido al traspaso entre celdas. Cada celda tiene una estación base que consiste en una torre y un pequeño edificio que contiene el equipo de radio.

2.2.1.1. Historia

Martin Cooper fue una de las primeras personas que desarrolló esta tecnología, es considerado como "el padre de la telefonía celular" ya que introdujo el primer radioteléfono en el año de 1973 en los Estados Unidos mientras trabajaba en Motorola, pero no fue hasta el año de 1979 que la compañía *Nippon Telegraph And Telephone Corp* (NTT) lanzó el primer sistema comercial en Tokio, Japón. En el año de 1981 se introduce en los países nórdicos un sistema celular semejante al *Advanced Mobile Phone System* (AMPS). Por otra parte, la entidad reguladora de Estado Unidos adopta reglas para crear un servicio de comercialización de la telefonía celular, gracias a esto en octubre del año 1983 se lleva a cabo el primer sistema de comercialización en la ciudad de Chicago. Desde entonces se extendió en varios países la telefonía celular como una gran alternativa a la telefonía alámbrica convencional. Se puede decir que la telefonía inalámbrica tuvo una acogida muy buena, es así que a los pocos años de haberse implantado el servicio, el mismo empezó a saturarse. Surgió entonces la necesidad de buscar nuevas formas de acceso múltiple al canal de comunicación, así como también la transformación de los sistemas analógicos a digitales con el fin de dar cabida a más usuarios. Existen varias etapas en la historia de la telefonía celular, las mismas que se

han categorizado en generaciones. A continuación se presentan cada una de ellas [18].

2.2.1.2. Sistemas de primera generación

Los sistemas de primera generación son sistemas analógicos, los mismos que fueron diseñados en Estados Unidos, Europa y Japón en la década de los años setenta. El sistema *Total Access Communications System* (TACS), fue creado en el Reino Unido; este sistema está relacionado al sistema estadounidense AMPS, el sistema *Nordic Advanced Mobile System* (NMTS), fue creado en los países escandinavos, y el sistema *Nippon Advanced Mobile Telephone Service* (NAMTS), se desarrolló en Japón. Todos estos sistemas están basados en el mismo principio de funcionamiento, aunque son sistemas incompatibles entre sí [19].

Los sistemas celulares de primera generación trabajan en dos bandas de frecuencia, una banda para el enlace ascendente, es decir la comunicación desde el terminal móvil hasta la estación base; y la otra banda para el enlace descendente, es decir la comunicación desde la estación base hasta el terminal móvil. Estas dos bandas de frecuencia varían según el sistema utilizado, pero están alrededor de los 900MHz, el ancho de banda utilizado por los enlaces ascendente y descendente depende del sistema con el que se trabaja, pero están alrededor de los 25MHz, este ancho de banda se divide en otros canales que se ocupan cuando se establece la comunicación. El ancho de cada uno de estos nuevos canales es de 25 o 30KHz y de 12,5KHz en el sistema NMTS, por lo que el número total de canales asignados a cada sistema es de aproximadamente mil canales. Este grupo de canales se divide para las estaciones base, de modo que una estación base y su vecina no tienen el mismo grupo de canales para así evitar interferencias [19].

2.2.1.3. Sistemas de segunda generación

Los sistemas de telefonía celular aparentemente prometían una capacidad que parecía ilimitada a partir de las subdivisiones en las celdas, pero a finales de los ochenta a medida que el tiempo avanzaba y la telefonía móvil se volvía más popular la industria de las telecomunicaciones se encontró con varias limitaciones prácticas. Económicamente construir celdas de menor tamaño resultaba difícil y poco factible, se hizo mas complicado ubicar las estaciones base en las nuevas zonas que las requerían, también debido a la saturación e interferencia en las celdas empezaron a darse limitaciones de capacidad. Por estas razones mencionadas las capacidades que se plantearon en los sistemas de primera generación no fueron adecuadas para satisfacer la demanda del mercado [19].

Por otra parte, un aspecto también importante, era la incompatibilidad de estánda-

res utilizados en Europa, lo que imposibilitaba el uso del teléfono celular en diferentes países. Debido a todas estas limitaciones se necesitaba crear un sistema de segunda generación para conseguir una mayor capacidad y la compatibilidad de los sistemas que operaban en diferentes países.

Para realizar el sistema de segunda generación, se decidió escoger una tecnología digital frente a la tecnología analógica utilizada en los sistemas de primera generación, los aspectos en los que la tecnología digital era superior a la analógica son los siguientes [19]:

- Técnicas de modulación digital.
- Las tasas de codificación de voz eran más reducidas.
- Técnicas de codificación de canal y entrelazado.
- El cifrado de las comunicaciones y la seguridad.
- Reducción del costo de la señalización.

Al utilizar los sistemas digitales se tiene como gran ventaja el poder abrir las puertas a nuevos servicios adicionales y de valor agregado como son los mensajes de texto cortos, el buzón de voz, el correo electrónico y servicios de gestión de llamadas [19].

2.2.1.4. Sistemas de tercera generación

Se preveía que para los primeros años del siglo XXI pudieran existir más de 300 millones de teléfonos celulares en todo el mundo. Estos usuarios harían uso no solo de los servicios de voz, sino también de otros servicios como el acceso a redes del tipo *Local Area Network* (LAN), acceso a Internet, correo electrónico, envío y recepción de imágenes de calidad, y hasta del servicio de video conferencia. Para poder hacer uso de esos servicios el ancho de banda de las redes celulares se debía incrementar, lo cual sucedió con las modificaciones de los estándares *Global System for Mobile Communications* (GSM), Estándar Interno (IS)-95 e IS-94. Estos sistemas podían soportar servicios de conmutación de circuitos y paquetes con velocidades de hasta aproximadamente 384Kbps. Para incrementar aun más estas velocidades fue necesario la creación de nuevas técnicas de acceso las cuales permitían soportar velocidades de hasta 2Mbps [19]. Al implementarse la tecnología *High Speed Packet Access* (HSPA) fue posible ofrecer velocidades de transmisión de hasta hasta 14.4Mbps en el enlace descendente y 5.8Mbps en el enlace ascendente. HSPA es un conjunto de protocolos de telefonía móvil que amplían y mejoran el rendimiento del protocolo *Universal Mobile Telecommunications System* (UMTS) ya existente [20].

La tecnología 3G permite a los operadores de red ofrecer a los usuarios una amplia gama de servicios avanzados y una mejor capacidad de la red a través de una mayor eficiencia espectral. La eficiencia espectral se refiere a la cantidad de información que puede ser transmitida sobre un ancho de banda dado en un sistema de comunicación digital específico [20].

3G tiene las siguientes mejoras sobre redes 2G y anteriores [20]:

- Audio mejorado y transmisión continua de vídeo.
- Velocidades de datos mucho mayores.
- Video conferencia.
- Acceso a Internet y Protocolo de Aplicaciones Inalámbricas (WAP) en mayores velocidades.
- Televisión por Internet (IPTV).

2.2.1.5. Sistemas de cuarta generación

La tecnología 4G se refiere a la cuarta generación de estándares inalámbricos celulares es el sucesor de 3G y 2G.

En esta se implementan redes *Internet Protocol* (IP) de conmutación de paquetes en banda ancha de ultra acceso y de transmisión multiportadora [20]. Se trata básicamente de la extensión de la tecnología 3G pero con mayor ancho de banda y mas servicios. Algunas empresas ofrecen la tecnología 4G a 100 Mbps para usuarios móviles, y hasta 1 Gbps para estaciones fijas [20].

2.2.2. Componentes básicos de los teléfonos celulares

La placa de circuito impreso *Printed Wiring Board* (PWB) de un teléfono celular es el cerebro del mismo; controla todas sus funciones y contiene los componentes electrónicos. PWB en general, se compone un tercio de cerámica y vidrio, un tercio plásticos, y un tercio de metales. Los fabricantes cada vez incorporan una variedad de funciones en sus productos, en los teléfonos móviles se han podido incorporar una creciente variedad de funciones en un espacio relativamente pequeño. Este cambio está provocando una rápida miniaturización de los teléfonos celulares. Los terminales de telefonía celular se componen generalmente de las siguientes unidades o componentes [21]:

- Carcasa
- PWB
- Antena

- Pantalla
- Teclado
- Micrófono
- Altavoz
- Batería

2.2.3. Sistemas operativos de teléfonos inteligentes

A medida que avanza la tecnología, los teléfonos móviles se han convertido en un aparato cada vez más sofisticado. Estos no sólo pueden hacer llamadas telefónicas desde cualquier lugar, también pueden enviar textos, imágenes, vídeos y conectarse a Internet. Los más recientes avances en los teléfonos celulares son los teléfonos inteligentes, que son capaces de muchas funciones diferentes, incluyendo el envío y recepción de correo electrónico, escuchar música, y descargar aplicaciones. Con el aumento de las capacidades de los teléfonos, los usuarios deben ser conscientes de las medidas de información y de seguridad necesarias [22].

Un Sistema Operativo Móvil (OS-móvil) es una plataforma de software sobre la que otros programas llamados programas de aplicación, se pueden ejecutar en dispositivos móviles como Asistente Personal Digital (PDA) , las tabletas, los teléfonos celulares, teléfonos inteligentes, etc. Durante todo el proceso, la arquitectura del sistema operativo móvil ha pasado de complejo a simple y ahora algo intermedio. El proceso de evolución es impulsado de forma natural por los avances tecnológicos en *hardware*, *software* e Internet. Los avances tecnológicos antes mencionados han dado lugar a una gran variedad de soluciones de sistema operativo para móviles que compiten en el mercado impulsados por diferentes actores. Algunos de estos actores son los siguientes [23]:

2.2.3.1. Android OS

Sistema operativo Android para dispositivos móviles desarrollado por la *Open Handset Alliance*, la cual es liderada por Google. Google dió a conocer la distribución de Android en noviembre de 2007. La mayor parte del núcleo de Android es liberado bajo código abierto *Apache License*, pero una gran cantidad de software en los dispositivos Android (como por ejemplo, *Play Store, Google Search, Google Play Services, Google Music*, etc.) son propietario y con licencia. A partir de 2011, Android tiene la mayor base instalada de cualquier sistema operativo móvil y a partir de 2013, sus dispositivos se vendieron más que los dispositivos Windows, iOS y Mac OS combinados. A partir de julio de 2013, la tienda de *Google Play* ha tenido más de 1 millón de aplicaciones de

Android publicadas y más de 50 mil millones de aplicaciones descargadas. Una encuesta realizada entre abril y mayo 2013 encontró que el 71 % de los desarrolladores móviles desarrollan para Android [23].

Android utiliza un *kernel* de Linux con las Interfaz de Programación de Aplicaciones (API) de alto nivel escritos en C y las aplicaciones que normalmente se programan en Java y corren con la Máquina Virtual Dalvik (DVM) mediante la compilación "justo a tiempo" para traducir el código de *bytes* de Java en Dalvik a código dex . Esta combinación trae algunas características seguras, como la gestión de la memoria compartida eficiente, multitarea preventiva,Identificador de Usuario Unix (UID) y los permisos de archivos con el concepto de seguridad de tipo Java. Cada aplicación Android corre en un proceso separado bajo un UID único con permisos distintos, lo que significa que las aplicaciones normalmente no pueden leer o escribir datos o código de cada uno. Para hacer que los recursos sean compartidos entre las aplicaciones posibles, los permisos que se requieren deben ser declarados de forma estática en el momento de instalar la aplicación. El sistema Android solicita al usuario su consentimiento en este momento; un mecanismo para la concesión de permisos de forma dinámica en tiempo de ejecución no es posible y daría lugar a un aumento de la transparencia de seguridad [23]. La plataforma Android contiene las capas que se pueden observar en la Figura 2.2.

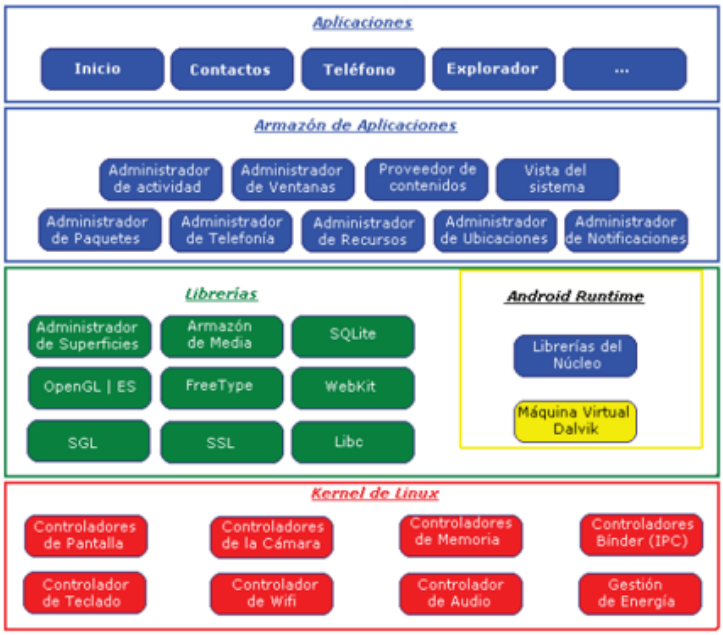


Figura 2.2: Arquitectura de Android OS. Fuente:[1].

2.2.3.2. iOS

iOS (antes iPhone OS) es un sistema operativo para móviles desarrollado por Apple Inc. y distribuido exclusivamente para el *hardware* de Apple. Es el sistema operativo que alimenta iPhone, iPad, iPod Touch y Apple TV. Es de código cerrado y propietario, construido en código abierto Darwin OS. iOS promueve un nuevo estilo de interacción del usuario para la pequeña pantalla, dispositivos de entrada limitadas, en concreto la manipulación directa. Acciones basadas en tecnología táctil como deslizar, tocar, tocar y mantener, pellizco se utilizan para el control de elementos de la interfaz de la pantalla, y para realizar operaciones de interfaz. Acelerómetros apoyan gestos físicos adicionales como agitación y la rotación de la orientación del dispositivo [23].

iOS se deriva de Mac OS X, y comparte su fundamento básico Darwin, un código abierto POSIX compatible con UNIX OS. En este sentido iOS se puede considerar una variante de UNIX. iOS se compone de cuatro capas de abstracción: *Core OS, Core Services, media, y Cocoa Touch,* como se observa en la Figura 2.3

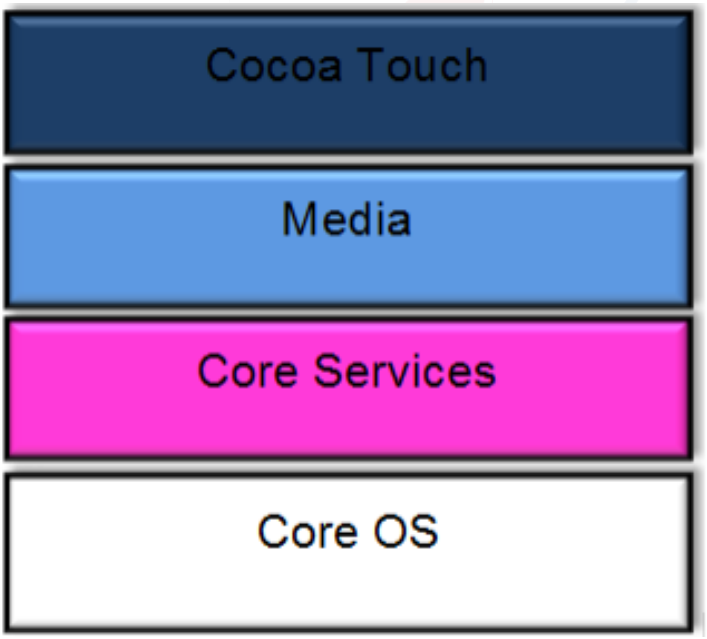


Figura 2.3: Arquitectura de iOS. Fuente:[2].

2.2.3.3. Windows Phone

Windows Phone es un sistema operativo propietario para teléfonos inteligentes desarrollado por Microsoft. Es el sucesor de Windows Mobile, a pesar de que es incompatible

con la plataforma anterior. Fue lanzado en 2010 bajo el nombre de Windows Phone 7. Varios fabricantes de *hardware* incluyendo HTC, Samsung, LG y Nokia están desarrollando dispositivos Windows Phone. En febrero de 2011 Nokia y Microsoft anunciaron que Windows Phone 7 sería el sistema operativo principal para todos los futuros teléfonos inteligentes de Nokia. Windows Phone 7 ha recibido una importante actualización (7.5 Mango) en febrero de 2011, la adición de características que habían sido desaparecidas en la versión original. La segunda generación de Windows Phone 8 fue lanzado en octubre de 2012. Actualmente la última actualización que existe es Windows Phone 10 [23]. La arquitectura de Windows Phone se puede observar en la siguiente Figura 2.4

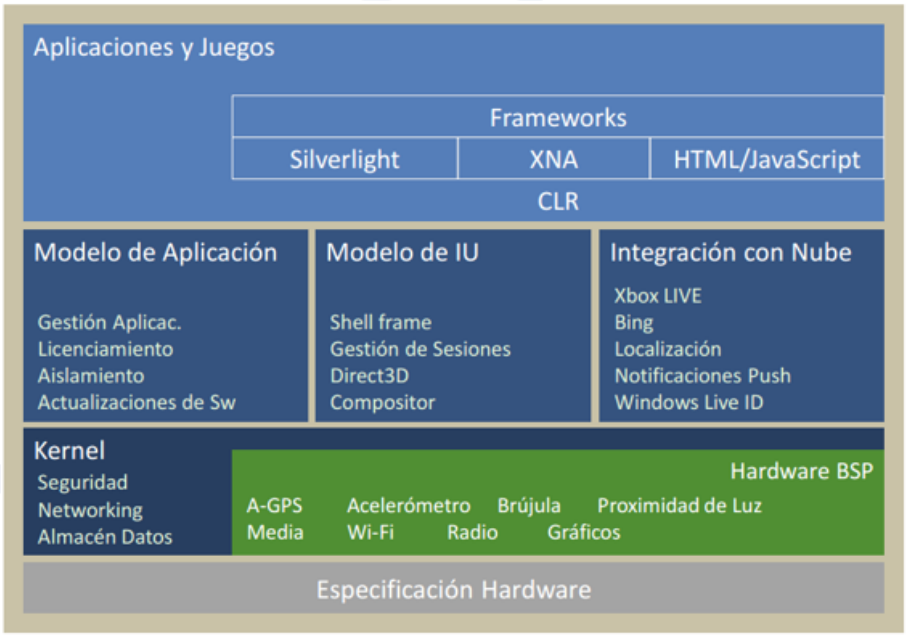


Figura 2.4: Arquitectura de Windows Phone. Fuente:[3].

2.2.3.4. Blackberry OS

BlackBerry OS es desarrollado por *Research in Motion* (RIM) para sus teléfonos inteligentes BlackBerry y dispositivos tablet. BlackBerry OS 1.0 debutó en enero de 1999 como parte de los dispositivos BlackBerry *pager/email*. Una de las principales fortalezas de los dispositivos BlackBerry es su capacidad para manejar el correo electrónico corporativo. BlackBerry OS es compatible con el *Mobile Information Device profile* (MIDP) de Java y WAP. Estos protocolos se utilizan para sincronizar a través

de un servidor *BlackBerry Enterprise Server* (BES) con el calendario basado en tareas, contactos, correo electrónico, y el intercambio de notas. BES ofrece la capacidad, seguridad, limpieza remota, y otras características que las empresas requieren para dispositivos móviles que acceden a las redes internas y/o datos corporativos. BlackBerry OS también proporciona *BlackBerry Internet Service* (BIS), un método específico del cliente para permitir el acceso a Internet para los usuarios individuales [23].

2.2.4. Potencial evidencia en dispositivos móviles

Uno de los efectos de la ley de Moore[1], es que ha habido una reducción masiva en el tamaño de los componentes junto con reducciones en la potencia requerida y precio. Esto ha creado oportunidades para el desarrollo de la tecnología personal portátil de bajo costo, que ha demostrado ser muy atractiva para el mercado de masas. Los dispositivos tales como teléfonos móviles, cámaras digitales, reproductores de medios digitales, sistemas de navegación por satélite y asistentes digitales personales han tenido significativa acogida desde su introducción, y es probable que sea justo decir que la mayoría de los hogares tiene al menos uno de estos dispositivos . En el fondo, cada uno de estos dispositivos es, en esencia, un micro ordenador y sigue los mismos principios de funcionamiento, pero los sistemas operativos y aplicaciones en estos dispositivos son a menudo altamente especializados, y pueden operar de tal manera que la extracción de datos y la interpretación no es tan sencilla que como en las computadoras de propósito general [5].

Hoy en día la gran mayoría de dispositivos móviles inteligentes cuentan con muchas características que son útiles en los diferentes campos tecnológicos, ya no hace falta comprar una cámara de video, un reproductor de música, etc, ya que muchos de estos dispositivos móviles llevan integrados todos estos elementos así como también un conjunto de sensores los cuales se pueden utilizar en aplicaciones con fines interactivos, tecnológicos, educativos, en salud, etc. Por lo que necesitan tener un lugar en donde almacenar toda la información, la mayoría de dispositivos móviles inteligentes están compuestos de dos memorias: una memoria interna que está dividida en dos partes, una parte de la memoria esta dedicada a las aplicaciones necesarias para que el dispositivo funcione como es el sistema operativo, la otra parte esta dedicada para almacenar los datos y la información, la otra memoria que dispone un móvil es la llamada memoria externa que es una tarjeta de memoria la cual se inserta al dispositivo y es completamente dedicada para el almacenamiento de la información. Por lo tanto se puede decir

[1]La ley de Moore afirma que el número de transistores por centímetro cuadrado en un circuito integrado se duplica cada año y medio [24].

que estos dos tipos de memoria son una potencial evidencia en el caso de un análisis forense; a continuación se presenta una revisión de algunos sensores de un teléfono inteligente, también se muestra como manipular los dos tipos de memorias ya antes mencionadas y finalmente un análisis del sitio en el que se encuentra un teléfono celular para su posterior manipulación.

2.2.4.1. Análisis de los sensores en un teléfono inteligente

Los teléfonos inteligentes modernos tienen varios tipos de sensores los cuales constituyen elementos tecnológicos que pueden considerarse como potencial fuente de evidencia digital; a continuación se presenta un análisis de los sensores utilizados en el presente proyecto como son: acelerómetro, giroscopio, magnetómetro, barómetro y GPS.

- Acelerómetro
  Un acelerómetro mide la aceleración que experimenta un cuerpo en relación con la caída libre, ésta es la aceleración sentida por personas y objetos. Para decirlo de otra manera, en cualquier punto en el espacio-tiempo el principio de equivalencia garantiza la existencia de un sistema inercial local y un acelerómetro mide la aceleración relativa a ese marco [4].
  El principio de funcionamiento del acelerómetro es usar la fuerza de inercia. Trate de imaginar una caja con seis paredes, una bola está flotando en el medio de la caja porque ninguna fuerza se añade a la pelota (por ejemplo, la caja puede estar en el espacio exterior). Cuando la caja se mueve hacia la derecha, la pelota golpea la pared izquierda. La pared de la izquierda es sensible a la presión que se puede medir por la fuerza aplicada al golpear la pared izquierda; por lo tanto, la aceleración puede ser medida. Debido a la gravedad, cuando la caja se coloca en la tierra, la pelota seguirá presionando la pared inferior de la caja y dará una aceleración constante de $9{,}8m/s^2$. La fuerza de la gravedad afectará a la medición del acelerómetro para medir la velocidad o el desplazamiento de un objeto en tres dimensiones. La fuerza de la gravedad se debe restar antes de una medición. Sin embargo, la fuerza de gravedad puede ser tomada como una ventaja para la detección de la rotación de un dispositivo. Cuando un usuario hace girar su teléfono inteligente, el contenido que está mirando va a cambiar entre vertical y horizontal. Como muestra la Figura 2.5, cuando la pantalla del teléfono inteligente está en condición vertical, el eje detectará la gravedad; cuando la pantalla del teléfono inteligente está en una condición horizontal, el eje detectará la gravedad. De acuerdo con esto, los usuarios pueden girar sus pantallas sin

afectar sus experiencias de lectura [4].

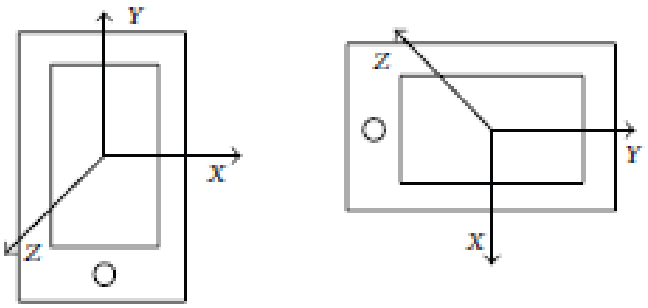


Figura 2.5: Rotacion de pantalla. Fuente:[4].

- Giroscopio
  Generalmente, un giroscopio es un dispositivo para medir o mantener la orientación, sobre la base de los principios de la conservación del momento angular. Un giroscopio (mecánico) convencional consiste en una rueda giratoria montada sobre dos cardanes que le permiten rotar en los tres ejes. Un efecto de la conservación del momento angular es que la rueda que gira resistirá los cambios de orientación. Por lo tanto cuando un giroscopio mecánico se somete a una rotación, la rueda se mantendrá en una orientación global constante y los ángulos entre los cardanes adyacentes cambiarán. Una orientación medida por el giroscopio convencional, en contraste con los tipos de *Micro Electro Mechanical System* (MEMS), que miden la velocidad angular, y por lo tanto se llaman *Rate*-giroscopios. Giroscopios MEMS contienen elementos de vibración para medir el efecto de Coriolis. Una sola masa es impulsada a vibrar a lo largo de un eje de accionamiento, cuando el giroscopio se hace girar se induce una vibración secundaria a lo largo del eje perpendicular debido a la fuerza de Coriolis. La velocidad angular puede ser calculada midiendo de esta rotación secundaria [25].
- Magnetómetro
  Un magnetómetro es un instrumento usado para medir la fuerza o dirección del campo magnético en la zona de los alrededores del instrumento. El magnetómetro se pueden dividir en dos tipos básicos: magnetómetros escalares que miden la fuerza total del campo magnético a la que están sometidos, y magnetómetros vectoriales, que tienen la capacidad de medir el componente del campo magnético en una dirección particular, en relación con la orientación espacial del dispositivo [25].

- Barómetro
  Tradicionalmente, el sensor barómetro se utiliza en meteorología para medir la presión atmosférica. También se utiliza como sensor de presión que mide la altitud relativa y absoluta a través del análisis del cambio de la presión atmosférica. El sensor barómetro se puede utilizar para la detección de movimiento, pero se utiliza sobre todo por las aplicaciones basadas en la localización para evaluar la elevación [26].
- GPS
  El GPS es un sistema de navegación por satélite desarrollado por el Departamento de Defensa de EE.UU. para fines militares. El sistema fue declarado plenamente operativo en 1994. Hoy en día el GPS se utiliza también con fines civiles, tales como topografía, diseño de mapas y obviamente navegación. El sistema GPS consta de tres segmentos; el segmento espacial (satélites), el segmento de control y el segmento de usuarios (receptores). El segmento espacial consta de 24 satélites que orbitan en seis órbitas que tienen una inclinación de 55° con respecto al ecuador. Las órbitas están dispuestas de tal manera que al menos seis satélites son siempre visibles desde todas partes en la superficie de la Tierra. Los satélites de GPS envían mensajes de navegación continuamente a una velocidad de 50 bits por segundo; la información principal del mensaje es el momento en que se envió el mensaje, la información exacta orbital, y el estado general del sistema y de las órbitas de todos los satélites en general. El segmento de control se compone de un número de estaciones y antenas, que se utilizan para controlar y supervisar el estado de los satélites, y hacer las correcciones necesarias cuando sea necesario, por ejemplo ajustar los relojes de los satélites. El segmento de usuario se compone de los usuarios militares del servicio de posicionamiento preciso GPS y los usuarios civiles del Servicio de Posicionamiento Estándar. El receptor GPS se compone principalmente de una antena, un reloj interno muy estable, el *software* para el cálculo de la ubicación y la velocidad del usuario, y por lo general una pantalla para proporcionar la información al usuario [25].

2.2.4.2. Memoria interna

La memoria interna de un dispositivo portátil es necesaria para cumplir dos funciones: debe funcionar como memoria principal tanto del dispositivo para la ejecución del sistema operativo, y como un sistema para almacenar archivos de datos. Muchos dispositivos proporcionan dos modos diferentes de funcionamiento cuando está conec-

tado a un ordenador: uno para la sincronización de los datos personales (por ejemplo diarios, correo electrónico, notas, etc.) y otro para la transferencia de archivos de datos. Es probable que ninguno de estos modos de hecho proporcione una imagen real de los contenidos de la memoria interna y puede que sea necesario, desmontar el dispositivo y conectarlo al equipo de diagnóstico especialista, o instalar un programa de recuperación de datos en el dispositivo. La instalación del programa de recuperación de datos, por supuesto, viola el Principio *Association of Chief Police Officers* (ACPO) 1[2] , porque implica la modificación del estado del dispositivo. Sin embargo, el Principio ACPO 2[3] permite que esto ocurra cuando la persona que realiza la instalación y el examen está calificado para dar una explicación de sus acciones. Cabe señalar que la memoria interna de estos dispositivos necesita en general ser más rápida y más flexible que la de almacenamiento extraíble y tiende a utilizar el mismo tipo de tecnología como la que se encuentra en las computadoras de escritorio y portátiles. Cuando se corta la energía, también se perderá el contenido de la memoria, aunque han sugerido estudios recientes en los cuales se menciona que puede ser posible acceder a los datos en la memoria volátil después de un período de unos pocos minutos, o más tiempo, incluso si la memoria es enfriada [5].

2.2.4.3. Memoria extraíble

La mayoría de los dispositivos modernos tienen una ranura en la que una tarjeta de almacenamiento de memoria se puede insertar en el dispositivo para ampliar el espacio de almacenamiento disponible y permitir el intercambio de datos con otros dispositivos. Estas tarjetas de memoria se ajustan a las mismas normas que en otros dispositivos con almacenamiento extraíble, y por lo general utilizan el mismo estándar de sistema de ficheros *File Allocation Table* (FAT) que se encuentra en esos dispositivos. Como resultado, el examen de las tarjetas de memoria se puede llevar a cabo utilizando herramientas estándar de examen de datos forenses. Se debe tener cuidado de asegurarse que el examinador sea consciente de cómo el sistema operativo del dispositivo se ocupa de las marcas de tiempo: de la última modificación, de la ultima escritura, de acceso y eliminación de archivos. Como dispositivos portátiles pueden exhibir comportamientos inusuales (por ejemplo, no establecer los tiempos de acceso, o borrar completamente

[2]Ninguna acción tomada por las agencias del orden las personas empleadas dentro de esos organismos o sus agentes debe alterar los datos almacenados en dispositivos electrónicos, los cuales posteriormente pueden ser de importancia en los tribunales [27].

[3]En circunstancias en las que una persona se ve obligado a acceder a los datos originales, esa persona debe ser competente para hacerlo y ser capaz de dar pruebas que aclaren la relevancia y las consecuencias de sus acciones [27].

los datos cuando hay un archivo suprimido), dando lugar a diferentes interpretaciones de sus contenidos y actividades. Afortunadamente, debido a que estos dispositivos de almacenamiento están diseñados para moverse entre los *hosts*, no pierden datos cuando se desconecta la alimentación y se puede tratar como discos duros para efectos de examinación, aunque un adaptador tal como el mostrado en la Figura 2.6 puede ser necesario para permitir que el software pueda leer los contenidos [5].

Figura 2.6: Lector de tarjetas de memoria extraíbles multi-formato conectado a través de un puente bloqueador de escritura forense. Fuente:[5].

2.2.4.4. Manejo de dispositivos celulares

En cuanto al manejo de dispositivos celulares, hay que tener presente que la constante interacción del teléfono con la red en la cual esta operando, representa una amenaza de consideración para la continuidad de las pruebas. Cualquier interacción del teléfono con la red después del descubrimiento del mismo puede dar lugar a la alteración del contenido del dispositivo. La información relacionada con la red a la que se conecta el dispositivo es importante ya que mediante la cartografía de intensidades de señal alrededor de una torre, es posible obtener un registro de las celdas usadas y en consecuencia, aproximar un mapa de la ruta que siguió el dispositivo [5].

La guía de buenas prácticas ACPO [27] para ordenadores, basada en la evidencia

electrónica, contiene recomendaciones detalladas sobre el manejo de los teléfonos celulares. El uso de jaulas de Faraday es muy recomendable para la captura, el transporte y la examinación de estos dispositivos, pero se debe recordar que un teléfono no puede ponerse en contacto con una celda, ya que intentará registrarse en la misma hasta que su fuente de alimentación se agote. Dado que las redes celulares utilizan diferentes frecuencias dependiendo del país, no se debe suponer que todas las jaulas de Faraday aislarán el teléfono de todas las redes. Distintas jaulas de Faraday tendrán diferentes niveles de permeabilidad para las distintas frecuencias [5]. El estándar *International Organization for Standardization/International Electrotechnical Commission* (ISO/IEC) 27037 menciona que al usar una jaula o bolsa de Faraday, u otros envases que protejan o mitiguen los efectos relacionados con la radio frecuencia, se puede aumentar el consumo de la batería del teléfono móvil. Esto puede requerir que exista un suministro de energía auxiliar para el dispositivo dentro de la bolsa si los recursos lo permiten [16].

2.2.5. Estado del arte

A continuación se presentan un conjunto de estudios relacionados con la temática de la presente investigación. Estos trabajos académicos fueron de gran ayuda para el cumplimiento de los objetivos propuestos en este proyecto. Se puede decir que constituyeron una guía y una fuente de información sobre los ejes principales de este estudio, en específico, sobre la adquisición de los datos de los sensores de sistemas electrónicos inerciales presentes en teléfonos inteligentes y otros dispositivos con el fin de obtener información suficiente y adecuada sobre la actividad motriz de un usuario, sobre el procesamiento y análisis de los datos adquiridos, y sobre la reconstrucción gráfica de la trayectoria que siguió un individuo.

2.2.5.1. Adquisición de datos

En la investigación *"Activity Recognition using Cell Phone Accelerometers"* realizada por el Departamento de Computación y Ciencias de la Información de la Universidad de Fordham [28], los autores se valieron de veintinueve personas voluntarias para realizar el proceso de adquisición de los datos con el fin de identificar un conjunto de actividades específicas a partir de las lecturas del acelerómetro de un teléfono inteligente. Todas las personas contaban con un teléfono inteligente con sistema operativo Android, y se les pidió colocar el dispositivo en el bolsillo delantero del pantalón. Las actividades realizadas por las personas eran básicamente: caminar, correr, subir escaleras, bajar escaleras, sentarse y estar de pie durante períodos determinados de tiempo. Los

datos fueron adquiridos mediante una aplicación creada por los autores de la investigación, ésta se ejecutaba en el teléfono mientras las personas realizaban las actividades específicas anteriormente descritas y contaba con una sencilla interfaz gráfica de usuario la cual les permitía registrar el nombre de cada voluntario, seleccionar la actividad realizada en cada periodo de tiempo y contaba además, con controles para iniciar y parar la adquisición de datos. Mediante la aplicación, los autores lograron obtener datos de sensores específicos como el acelerómetro o el GPS del teléfono inteligente, así como la frecuencia con la que estos eran registrados o almacenados. En todos los casos los autores utilizaron una periodo de muestreo de 50ms para obtener los datos de los sensores, dando un total de 20 muestras por segundo.

En *"An Ensemble Approach for Activity Recognition with Accelerometer in Mobilephone"*, investigación realizada por la Facultad de Informática e Ingeniería de Control de la Universidad de Nankai [29], se lleva a cabo el reconocimiento de actividades diarias. Los autores de la investigación optaron por el sistema operativo Android en un teléfono móvil Xiaomi 2S para la adquisición de los datos del acelerómetro. Realizaron una aplicación la cual tenía la función de activar los sensores del teléfono móvil. Para la investigación se contó con 9 personas voluntarias, las cuales colocaron el teléfono móvil en diferentes partes del cuerpo, se les solicitó que por un periodo de tiempo determinado realicen cinco actividades diarias, las cuales eran: caminar, correr, mantenerse de pie, subir y bajar escaleras. Al momento de realizar las actividades el acelerómetro adquiría los datos en los tres ejes (x,y,z) a una frecuencia especificada de 100Hz.

El Departamento de Ciencias Informáticas e Ingeniería de la Universidad de Oulu en Finlandia, realizó la investigación que lleva por título *"Recognizing Human Activities Userindependently on Smartphones Based on Accelerometer Data"* [30]. El objetivo de la misma fue el reconocimiento de cinco actividades diferentes. En la investigación los autores realizan la adquisición de datos mediante un teléfono inteligente Nokia N8 con sistema operativo Symbian3. Los datos para poder entrenar los modelos utilizados fueron tomados del acelerómetro en ocho personas cuya edad variaba de 25 a 34 años (promedio 29 años) y con una altura de 1.65 a 1,90 metros (media 1,78 metros), a las mismas que se les pidió colocar el teléfono celular en el bolsillo delantero del pantalón, ya sea el derecho o el izquierdo y realizar cinco actividades diferentes las cuales eran: caminar, correr, montar en bicicleta, conducir un coche, e inactividad, es decir, sentado o de pie. Los datos recolectados fueron de un periodo de cuatro horas aproximadamente y se utilizó el acelerómetro con una frecuencia de muestreo de 40Hz. Las actividades que realizaron las personas se llevaron a cabo fuera del laboratorio. Las actividades de caminar y correr no solo se realizaron en superficies planas sino también en gradas. Al

momento de conducir bicicleta y el coche se utilizaron carreteras asfaltadas.

Por otra parte, en la investigación "Estimación de posición de viandantes mediante sensores inerciales" [31], los autores utilizaron la unidad inercial *Motion Trackers* (MTi) de *Xsens Technologies*, y su variante MTi-G que es un pequeño sistema que integra diversos sensores en miniatura, como acelerómetros, giroscopios, brújula y barómetro, para realizar la adquisición de datos. Dicho sistema fue colocado en el empeine del pie de una persona mientras esta caminaba, y los datos obtenidos fueron las variaciones de aceleración en los tres ejes del dispositivo, velocidades angulares, intensidad de campo magnético y orientación con respecto a un sistema de referencia de coordenadas (pitch, roll y yaw).

En *"Spoof Attacks on Gait Authentication System"* [32], los autores llevan a cabo una investigación acerca de los posibles ataques a un sistema de seguridad que identifica a los individuos por su forma de caminar, estos ataques se realizan imitando la forma de caminar de una persona en específico. Con el fin de obtener los rasgos característicos del caminar de una persona, los autores decidieron utilizar un dispositivo ubicado en la cadera de un individuo, este dispositivo no es más que un sensor de movimiento constituido por tres acelerómetros, una memoria de 64 *megabytes* para el almacenamiento de los datos obtenidos, interfaces para la transferencia de datos y una batería. En esta investigación los únicos datos obtenidos son aquellos referentes a las aceleraciones del dispositivo cuando una persona camina.

Otra aplicación basada en la utilización de sensores inerciales se describe en la investigación *"Identification of Pressed Keys From Mechanical Vibrations"* [33], en la que se identifica una secuencia de pulsación de teclas. Los autores realizan la adquisición de datos mediante la colocación de tres acelerómetros en la parte inferior del teclado. Cabe mencionar que para cada pulsación los acelerómetros obtenían tres vectores con 300 valores cada uno, los mismos que pertenecían a la aceleración en los tres ejes (x,y,z).

2.2.5.2. Procesamiento y análisis de datos

En [28], con el fin de diferenciar cada uno de los movimientos, los autores obtuvieron características informativas de un conjunto de datos. Cada conjunto de datos estaba constituido por la recopilación de 200 muestras del acelerómetro, cada muestra contenía valores de los ejes x, y, z. Las características informativas que se obtuvieron para la diferenciación de las seis actividades fueron: la media, la desviación estándar, la diferencia absoluta media, la aceleración resultante media, tiempo entre los picos y distribuciones agrupadas.

De igual forma en [34] para la tarea de reconocimiento de actividad, se utilizó un conjunto de características en el dominio del tiempo y de la frecuencia. En el dominio del tiempo fueron la media de la magnitud de la aceleración resultante, la varianza de la magnitud de la aceleración resultante, la desviación estándar (para cada eje del acelerómetro). En el dominio de la frecuencia se utilizaron los coeficientes de la *Fast Fourier Transform* (FTT), estos coeficientes fueron útiles en la detección de la periodicidad de las actividades ya que algunas de las actividades realizadas son repetitivas o periódicas como es el caminar, correr, subir y bajar escaleras.

Mientras que en [32], una vez obtenidos los datos registrados por el dispositivo referentes a las acelaraciones en los tres ejes (x,y,z) cuando una persona camina, se realiza una transformación que deja en términos de la gravedad a estos valores. Posteriormente se obtiene la magnitud de la aceleración resultante para cada conjunto de muestras del experimento. A partir de la realización de varios ensayos, los autores finalmente logran obtener un experimento de muestra que es la media de las aceleraciones resultantes de todos los experimentos. Este experimento de muestra puede ser comparado con posteriores experimentos de prueba para así poder identificar a una persona.

Para poder realizar la clasificación de las teclas pulsadas en [31], después de probar con varios algoritmos de aprendizaje automático los autores optaron por la utilización de dos algoritmos los cuales fueron: el perceptrón multicapa y el *Support Vector Machine* (SVM). Para poder entrenar a los mismos se realizó la *Zero-Normalized Cross Correlation* (NCC) entre los vectores de datos obtenidos por los acelerómetros. La NCC se ha utilizado por mucho tiempo en la visión artificial para poder clasificar y categorizar imágenes. Ya que el vector resultante de NCC tiene demasiados elementos y no es posible entrenar a los algoritmos de aprendizaje con todos estos elementos, los autores optaron por utilizar solo los elementos más significativos de los vectores compuestos por los datos otorgados por los acelerómetros.

2.2.5.3. Reconstrucción gráfica de la trayectoria

En *"Implementing Positioning Algorithms Using Accelerometers"* [35], una guía para la implementación de algoritmos de posicionamiento usando acelerómetros, se realiza una doble integración numérica de los datos obtenidos para obtener la posición del dispositivo inercial. Los autores utilizan este método basándose en el sustento matemático de que la aceleración no es más que la variación de la velocidad de un objeto, y a su vez, la velocidad no es más que la variación de la posición de un objeto en el tiempo. Es decir, la aceleración es la segunda derivada de la posición de un objeto con respecto al

tiempo, por lo que teóricamente sería posible obtener la posición del dispositivo inercial sabiendo únicamente su aceleración, sin embargo, los autores recalcan que la utilización de este método introduce errores acumulativos debido a que la integración utilizada es del tipo numérico y no una integral definida. Con el fin de minimizar el error generado los autores optan por utilizar el método trapezoidal para la integración numérica.

De igual forma, en [31], los autores se percatan de este error de carácter acumulativo y optan por desarrollar un mecanismo de corrección que se basa en los valores de las velocidades angulares del dispositivo. Además, con el objetivo de determinar la dirección del movimiento del sensor inercial, los autores se valen de los datos proporcionados por la brújula o el giroscopio. También recalcan que existen errores al momento de obtener los datos de estos dos últimos sensores. Para el caso de la brújula, sus mediciones se ven afectadas por entornos o elementos metálicos; mientras que para el caso del giroscopio, dado que los valores otorgados por el mismo son velocidades angulares, es nuevamente necesario realizar una integración numérica que introducirá un error que puede ser aceptable solo para cortos intervalos de tiempo. Finalmente en esta investigación se utilizan los datos provenientes del barómetro del dispositivo con el fin de determinar la altura a la que se encuentra el dispositivo, con estos últimos datos es posible realizar una recreación tridimensional de la trayectoria seguida por la persona que porta el sistema inercial.

2.2.5.4. Conclusiones

Se puede observar que en todas las investigaciones el acelerómetro es utilizado como elemento principal al momento de identificar la realización de una acción o movimiento determinado, por lo que se puede justificar el uso de los datos provenientes este sensor en la presente investigación para la detección de actividad motriz inusual. La frecuencia de muestreo es otro de los aspectos a tomar en cuenta, en varias investigaciones se recalca la importancia de establecer esta magnitud según el tipo de actividades que se desea identificar. En la mayoría de investigaciones presentadas en esta sección los autores utilizan un grupo de medidas estadísticas para caracterizar las diferentes actividades realizadas, este conjunto de características son utilizadas para el entrenamiento de algoritmos de aprendizaje automático. Estos algoritmos lo que hacen es realizar la clasificación de cada conjunto de características en las diferentes actividades que realizaron los sujetos de prueba. Lo anterior resulta muy útil para poder diferenciar entre actividades que se realizan muy a menudo, el problema sería intentar reconocer una actividad motriz inusual, es decir, una actividad que no se la realiza constantemente,

en este caso los algoritmos de clasificación carecen de validez. Finalmente, en cuanto al tema de la reconstrucción gráfica de la trayectoria, el error acumulativo obtenido debido a la utilización de una doble integración numérica para la obtención de la posición de una persona es de consideración, y a pesar de las correcciones que puedan realizarse este error siempre estará presente. Resulta necesario valerse de datos provenientes de otros sensores con el fin de cumplir con la tarea de reconstrucción.

Capítulo 3

Aplicación móvil para la adquisición de eventos

La aplicación desarrollada está destinada para el funcionamiento en teléfonos inteligentes que cuentan con el sistema operativo Android, y se implementó enteramente en Android Studio que es el *Integrated Development Environment* (IDE) oficial para el desarrollo de aplicaciones Android. La aplicación recopila información sobre el dispositivo como su aceleración, ubicación geográfica, orientación, conteo de pasos, altitud, hora y fecha. A partir de toda esta información es posible realizar la detección de actividad motriz inusual así como la reconstrucción gráfica de los hechos en el SS. La interfaz gráfica de la aplicación en funcionamiento se presenta en la Figura 3.1. Resulta conveniente acotar que, aunque se presentan varias de las lecturas de los sensores en la interfaz gráfica, existen otros datos de gran importancia como la latitud y longitud de la ubicación geográfica obtenidos del GPS, que no se muestran pero que igualmente son almacenados para su posterior procesamiento y análisis. El mostrar en pantalla varios de los datos obtenidos, tiene como única finalidad, otorgar a los investigadores un medio visual para la comprensión adecuada del funcionamiento de los sensores y métodos utilizados en la aplicación, por lo que en versiones futuras de la aplicación no sería necesaria la visualización de dicha información. A continuación se detalla el funcionamiento general de la aplicación móvil a partir de su diseño e implementación.

Figura 3.1: Interfaz gráfica de la aplicación desarrollada.

3.1. Diseño

De acuerdo con los objetivos planteados en la presente investigación, es necesario llevar a cabo tanto la detección de actividad motriz inusual así como la reconstrucción gráfica de dicha actividad en el SS. La realización de ambas tareas se basa en la obtención de un conjunto específico de datos provenientes de un teléfono inteligente. Los datos necesarios para cada una se detallan en la tabla 3.1:

Detección de actividad motriz inusual	**Reconstrucción gráfica de los hechos**
Acelerómetro	Orientación
	Contador de pasos (Desplazamiento horizontal)
	Altímetro (Desplazamiento vertical)
	GPS
Hora y fecha	

Tabla 3.1: Datos utilizados para cada tarea.

Para el caso de la detección de actividad motriz inusual está claro que únicamente se requiere adquirir y almacenar los datos del acelerómetro, sin embargo, es necesario llevar a cabo un procesamiento de estos en tiempo real, es decir, en el mismo teléfono inteligente cuando la aplicación se encuentra en ejecución. Lo anterior tiene que ver con

la adquisición de información proveniente del GPS del dispositivo, esta información no puede ser registrada de forma continua ya que constituye una violación a la privacidad de la víctima, es así que se ha restringido su almacenamiento únicamente para cuando se producen lecturas del acelerómetro que indican la realización de algún tipo de actividad abrupta.

La forma en la que se determina la ocurrencia de actividad inusual es mediante la comparación de los datos del acelerómetro, específicamente la aceleración resultante, con un valor umbral. Se puede observar en detalle los pasos del procesamiento en tiempo real en el diagrama de flujo de la Figura 3.2. Los datos del GPS son de considerable importancia ya que mediante estos se puede ubicar a la víctima y al SS.

Figura 3.2: Procesamiento en tiempo real para la adquisición de datos del GPS.

Con respecto a la reconstrucción gráfica de los hechos, y dado que dicha recreación se llevará a cabo en tres dimensiones, resulta indispensable obtener información acerca de la orientación del dispositivo y su desplazamiento tanto horizontal como vertical (véase

Figura 3.3), además de los datos del GPS necesarios para ubicar geográficamente al SS.

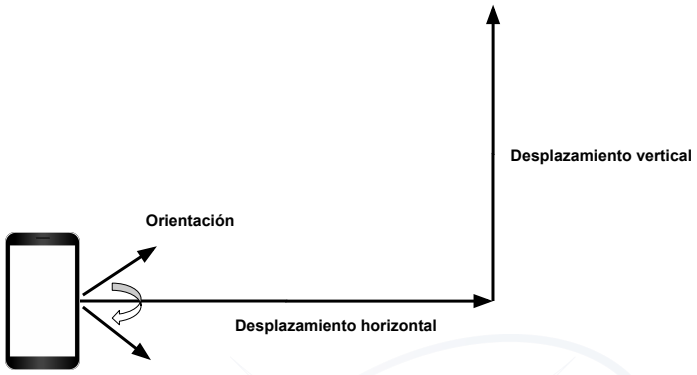


Figura 3.3: Datos necesarios para la reconstrucción gráfica de los hechos en tres dimensiones.

Finalmente es necesario registrar cada una de las lecturas junto con la fecha y hora en los que se llevó a cabo la adquisición en el teléfono inteligente con el objetivo de ubicar temporalmente la ocurrencia de cualquier tipo de actividad motriz inusual.

Todos estos datos deben ser almacenados continuamente por la aplicación a intervalos de tiempo constantes a excepción de los datos del GPS por las razones indicadas anteriormente. Se decidió que la forma más efectiva para el almacenamiento de este conjunto de información sea mediante dos archivos de texto localizados en la memoria interna del teléfono inteligente, de esta forma se garantiza el fácil acceso por parte de la aplicación de escritorio desarrollada en MATLAB para el procesamiento y análisis de los datos recopilados.

El constante almacenamiento de este conjunto de información en archivos de texto por periodos de tiempo prolongados, supone un constante incremento en la utilización de la memoria interna del dispositivo, por lo que es necesario optimizar el uso de la memoria disponible descartando aquellos periodos de tiempo en los que no se detectó algún tipo de actividad motriz inusual. Se estableció que el periodo de tiempo para el almacenamiento sea de una hora, luego de transcurrido este tiempo se comprobará si existió algún tipo de actividad inusual, si el resultado es afirmativo se conservarán los dos archivos, caso contrario la aplicación procederá con la eliminación de los mismos. Este proceso de optimización se representa mediante un diagrama de flujo en la Figura 3.4.

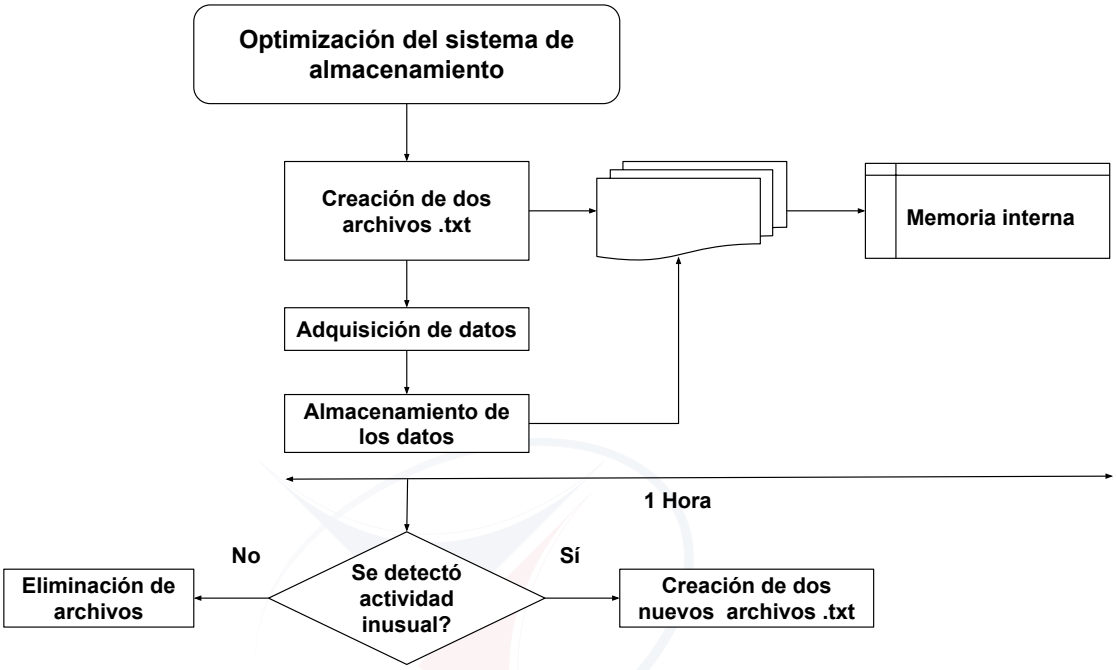


Figura 3.4: Proceso de optimización del sistema de almacenamiento de datos.

3.2. Implementación

El elemento principal en la implementación de la aplicación en Android Studio es la clase ***SensorManager***, mediante una instancia u objeto[1] de esta clase es posible acceder a los sensores del teléfono inteligente [36]. También es necesario crear un total de cuatro instancias de la clase ***Sensor*** correspondientes a los tipos de sensores necesarios para obtener los datos de aceleración, orientación, conteo de pasos y altura. En el sistema operativo Android existen varios tipos de sensores pertenecientes a la clase ***Sensor***, en la siguiente tabla se resumen los utilizados por la aplicación desarrollada:

Función	Sensor
Acelerómetro	*TYPE_LINEAR_ACCELERATION*
Orientación	*TYPE_ORIENTATION*
Contador de pasos	*TYPE_STEP_COUNTER*
Altímetro	*TYPE_PRESSURE*

Tabla 3.2: Tipos de sensores utilizados y su función.

[1] En el lenguaje de programación Java, un objeto constituye la instancia de una clase.

Otro elemento importante utilizado en la implementación de la aplicación es el método ***onSensorChanged***, este método es utilizado de forma general por los cuatro sensores presentados anteriormente con el fin de obtener los datos o valores provenientes de los mismos cuando la aplicación ha detectado un cambio en la magnitud de las mediciones. Cabe recalcar que este cambio de magnitud en los valores de cada sensor ocurre de acuerdo a un retraso en la adquisición definido previamente. El retraso determina el periodo de muestreo de los valores de cada sensor. De acuerdo a las consultas realizadas en [37], existen cuatro tipos de retraso predefinidos en Android que son utilizados de acuerdo al tipo de aplicación, cada uno con un retraso de tiempo específico. Lo anterior se resume en la Tabla 3.3.

Tipo	**Caso de uso**	**Tiempo (us)**	**Tiempo (ms)**
SENSOR_DELAY_FASTEST	Adecuado para obtener datos de los sensores lo más rápido posible	0	0
SENSOR_DELAY_GAME	Adecuado para juegos	20000	20
SENSOR_DELAY_NORMAL	Adecuado para cambios en la orientación de la pantalla	200000	200
SENSOR_DELAY_UI	Adecuado para la interfaz de usuario	60000	60

Tabla 3.3: Casos de uso y equivalencias temporales de los tipos de retraso para la adquisición de datos de los sensores.

Antes de continuar resulta necesario presentar el sistema de coordenadas utilizado por Android, es importante identificar y comprender dicho sistema ya que varios de los sensores se basan en el mismo para proporcionar diversos datos al sistema operativo. El sistema de coordenadas en cuestión (véase Figura 3.5) se define como relativo a la pantalla del teléfono inteligente, la posición de los ejes no depende de la orientación de la pantalla del dispositivo. El eje x es horizontal y apunta hacia la derecha, el eje y es vertical y apunta hacia arriba, y el eje z apunta hacia el exterior de la cara frontal de la pantalla. En este sistema, las coordenadas detrás de la pantalla tienen valores z negativos [6].

Cada uno de los sensores provee diferentes conjuntos de valores según la naturaleza de las mediciones que se pueden realizar con ellos, además existen ciertas características

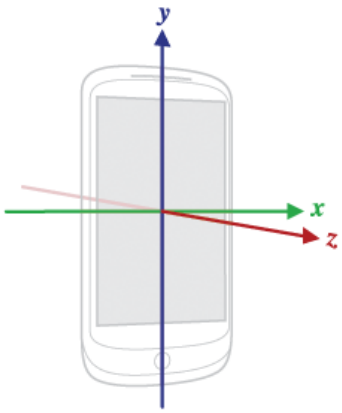


Figura 3.5: Sistema de coordenadas utilizado en Android. Fuente:[6].

y métodos propios de cada tipo de sensor. Con el afán de lograr un mayor entendimiento en cuanto a la implementación y funcionamiento de la aplicación, se detalla esta información a continuación.

- ***TYPE_LINEAR_ACCELERATION***
  De este tipo de sensor se obtienen en total tres valores correspondientes a las aceleraciones a lo largo de los ejes del dispositivo excluyendo la influencia de la gravedad. Para la implementación de la aplicación, es importante utilizar este sensor ya que al obviar la influencia del valor de la gravedad de la Tierra en los tres ejes, se puede detectar con un mayor grado de precisión cualquier tipo de actividad motriz inusual. Si no se obviara este valor, aunque el dispositivo se encuentre en reposo, la magnitud de la gravedad se verá reflejada en uno de los ejes del dispositivo dependiendo de su posición. Este sensor utiliza al acelerómetro del dispositivo y la unidad en la que se miden los tres valores es el m/s^2 [6].
- ***TYPE_ORIENTATION***
  De igual forma que el anterior, este tipo de sensor proporciona tres valores. Estos valores se miden en grados. El primero, denominado *Azimuth*, constituye el ángulo entre la dirección del norte magnético y el eje y, es decir, alrededor del eje z (0° a 359°). Siendo 0° = *Norte*, 90° = *Este*, 180° = *Sur*, 270° = *Oeste*. El segundo valor se denomina *Pitch* y el tercero *Roll*, estos miden la rotación alrededor del eje x y el eje y, respectivamente [6]. Para la posterior reconstrucción gráfica de la trayectoria que siguió el dispositivo únicamente se utiliza el primer valor por lo que solo este es tomado en cuenta para el análisis y procesamiento. Cabe recalcar, que este tipo de sensor utiliza una combinación de los datos provenientes del

magnetómetro y giroscopio del dispositivo con el fin de obtener los valores en grados descritos previamente [6].

- ***TYPE_STEP_COUNTER***
  Provee un solo número entero que representa la cantidad total de pasos dados por el usuario del dispositivo desde el último reinicio del sistema [38]. Con el objetivo de obtener el número de pasos dados desde que se ejecutó la aplicación y no desde el último reinicio, se creó una variable que aumenta en una unidad su valor cada vez que se detecta un cambio en la magnitud total, como se explicó anteriormente este cambio se detecta gracias al método ***onSensorChanged***.
- ***TYPE_PRESSURE***
  Mediante este sensor se obtiene un solo valor correspondiente a la presión atmosférica a la que se somete el dispositivo. Su unidad es el hPa [6]. Tal valor, no es almacenado por la aplicación sino que se utiliza en uno de los métodos de la clase ***SensorManager*** denominado ***getAltitude*** el cual devuelve una aproximación de la altura, en metros, sobre el nivel del mar a la que se encuentra el teléfono inteligente.

Otro de los recursos que se aprovechan del teléfono inteligente es el GPS. Los datos que se extraen de este sistema son dos, correspondientes a los valores de la latitud y la longitud de la posición geográfica en formato decimal. La aplicación accede a estos datos mediante instancias de las clases ***LocationManager*** y ***LocationListener***, no sin antes haberle otorgado permisos especiales y necesarios para que el sistema operativo Android le permita realizar esta tarea sin inconvenientes. Como se explicó en la sección de diseño de la aplicación, estos valores únicamente se obtienen al detectar un movimiento brusco por lo que se realiza un procesamiento en tiempo real tomando como elemento principal al cómputo de la aceleración resultante a partir de los datos del sensor ***TYPE_LINEAR_ACCELERATION***. La aceleración resultante se define como la raíz cuadrada de la suma de los cuadrados de las componentes de la aceleración, y matemáticamente se expresa como se muestra en la ecuación (3.2.1).

$$a_r = \sqrt{a_x^2 + a_y^2 + a_z^2} \tag{3.2.1}$$

La aplicación realiza este cálculo cada vez que se llama al método ***onSensorChanged***, y únicamente obtiene los datos del GPS si la aceleración resultante calculada es mayor o igual a 20 m/s^2. Más adelante se justifica el uso de este valor como parámetro de comparación, pero se puede adelantar que en general la aceleración resultante de un movimiento inusual, es siempre mayor o igual a esta magnitud.

Una vez obtenidos los datos requeridos del teléfono inteligente, la aplicación procede con el almacenamiento de los mismos en dos archivos de texto creados para este propósito. Estos dos archivos son creados en la carpeta ***Pictures*** del dispositivo con los nombres **"datosacelin0.txt**" y **"datosorientacion0.txt**" en las primeras etapas de ejecución de la aplicación. Se decidió diferenciar a los archivos mediante números, razón por la cual se aprecia el número 0 en los nombres de los primeros archivos (véase Figura 3.6) .

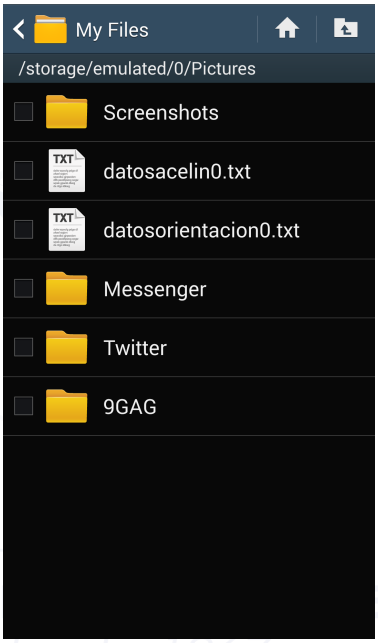


Figura 3.6: Primeros archivos creados por la aplicación y su localización.

La aplicación realiza la escritura en los archivos mediante una instancia de la clase ***FileOutputStream*** y su método ***write*** que utiliza como argumento de entrada una cadena de caracteres o *string*. Para almacenar los datos en el primer archivo, la aplicación crea una variable tipo *string* que se compone de los tres valores de la aceleración lineal, la altitud y longitud del GPS (solo al detectarse un movimiento brusco a partir del procesamiento en tiempo real ya explicado caso contrario almacena dos ceros en lugar de estos valores) y la fecha y hora del dispositivo. Todos estos elementos separados por medio de un espacio, y al final del *string*, se agrega un salto de línea para poder diferenciar cada registro (véase Figura 3.7), pero esta vez constituida por: los tres ángulos de orientación, el número de pasos dados de la ejecución de la aplicación y la altura aproximada sobre el nivel del mar.

```
-0.3611 -0.1479 0.9516 0 0 01:19:53 2016 02 29
-0.0296 -0.0637 0.9320 0 0 01:19:53 2016 02 29
-0.4240 -0.3046 0.9268 0 0 01:19:53 2016 02 29
-0.7824 -0.3499 1.2010 0 0 01:19:53 2016 02 29
-1.5505 -0.4801 1.2780 0 0 01:19:53 2016 02 29
-0.9036 -0.0725 0.3576 0 0 01:19:53 2016 02 29
-0.0178 0.0250 -0.7182 0 0 01:19:53 2016 02 29
-0.7851 -0.9656 -0.0363 0 0 01:19:53 2016 02 29
0.8851 -1.1933 1.8137 0 0 01:19:53 2016 02 29
7.2765 -0.0270 4.6864 0 0 01:19:53 2016 02 29
13.6759 4.5001 7.3137 0 0 01:19:53 2016 02 29
13.2529 8.0556 11.5850 0 0 01:19:53 2016 02 29
13.1743 3.6678 17.2581 -2.91579 -78.99233 01:19:53 2016 02 29
13.5498 -1.8554 17.6762 -2.91579 -78.99233 01:19:53 2016 02 29
14.3366 -7.3175 18.3560 -2.91579 -78.99233 01:19:53 2016 02 29
15.7107 -18.9825 18.0822 -2.91579 -78.99233 01:19:53 2016 02 29
15.0302 -29.1805 13.2495 -2.91579 -78.99233 01:19:53 2016 02 29
-0.1504 -29.1575 7.4616 -2.91579 -78.99233 01:19:53 2016 02 29
-8.5245 -28.5147 2.0609 -2.91579 -78.99233 01:19:53 2016 02 29
-15.6717 -27.3959 -3.4878 -2.91579 -78.99233 01:19:53 2016 02 29
-14.3294 -26.1812 -4.2016 -2.91579 -78.99233 01:19:53 2016 02 29
-13.6555 -25.2715 -2.7663 -2.91579 -78.99233 01:19:53 2016 02 29
-13.3194 -24.5078 -2.1503 -2.91579 -78.99233 01:19:53 2016 02 29
-13.2946 -19.7922 -7.6174 -2.91579 -78.99233 01:19:53 2016 02 29
-13.3402 -18.0209 -8.5289 -2.91579 -78.99233 01:19:53 2016 02 29
-8.9351 -18.3868 -8.7093 -2.91579 -78.99233 01:19:53 2016 02 29
-4.4282 -20.5943 -4.4054 -2.91579 -78.99233 01:19:53 2016 02 29
5.5993 -2.9008 -0.2088 0 0 01:19:53 2016 02 29
18.4418 4.3484 8.3445 -2.91579 -78.99233 01:19:53 2016 02 29
25.6470 11.6064 16.0456 -2.91579 -78.99233 01:19:53 2016 02 29
```

Figura 3.7: Información almacenada en el archivo “datosacelin0.txt”.

Para el almacenamiento de información en el segundo archivo se crea otra variable tipo *string* pero esta vez constituida por: los tres ángulos de orientación, el número de pasos dados desde la ejecución de la aplicación y la altura aproximada sobre el nivel del mar; de igual forma todos estos elementos se separan por un espacio y se agrega un salto de línea al final de la cadena de caracteres (véase Figura 3.8).

Finalmente, la aplicación detecta el paso de una hora en su ejecución mediante el método ***nanoTime*** el cual devuelve el tiempo en nano segundos desde el último reinicio del sistema. Se crean dos variables que almacenan este valor, la primera al inicio de la aplicación y una segunda que se actualiza constantemente cuando se almacena la información en los archivos, mediante su diferencia y transformando la misma a segundos, se realiza una comparación con el valor de 3600 segundos que equivalen a una hora. Debido a que es necesario realizar la optimización del sistema de almacenamiento, durante el procesamiento en tiempo real, se crea un contador que determina el número de veces que la aceleración lineal resultante fue mayor a 20 m/s^2, es decir, el número de veces que ocurrió un movimiento brusco. Si el valor del contador es igual a 0, se eliminan los dos archivos correspondientes a la hora transcurrida en ese momento; mientras que si su valor es mayor que 0, la aplicación no elimina los archivos y crea dos nuevos con nombres distintos a los anteriores para el almacenamiento de nueva información. Se puede decir que este proceso realiza la creación o eliminación de archivos recursivamente

```
293.3445 -32.4326 32.4384 9.0000 2392
296.5863 -31.0406 29.7960 9.0000 2392
297.7086 -30.6781 29.0552 9.0000 2392
301.5057 -40.3246 24.9214 9.0000 2393
305.3810 -47.7003 20.0004 9.0000 2393
311.6351 -53.4883 12.1018 9.0000 2393
313.3460 -56.1777 11.1960 9.0000 2393
310.2972 -56.2857 11.2679 9.0000 2393
306.2568 -54.8325 12.2086 9.0000 2393
73.4275 -178.2857 -56.6395 10.0000 2393
73.6696 -177.7926 -55.0972 10.0000 2393
44.1716 -171.1702 -57.0389 10.0000 2393
16.1645 -167.8258 -50.5894 10.0000 2393
7.5647 -159.7471 -52.9271 10.0000 2393
8.3669 -152.4232 -55.0835 10.0000 2393
6.9339 -147.8904 -56.4997 10.0000 2393
6.9102 -145.4272 -57.0316 10.0000 2393
305.6175 -41.7120 15.5095 10.0000 2393
308.0468 -42.4305 14.1899 10.0000 2393
310.2172 -43.1371 13.6333 10.0000 2393
311.3605 -42.8454 13.7493 10.0000 2393
311.7046 -42.8650 14.6959 10.0000 2392
```

Figura 3.8: Información almacenada en el archivo “datosorientacion0.txt”.

al cabo de una hora a partir de comparaciones con la diferencia de tiempos y el contador definidos previamente. En la Figura 3.9 se puede apreciar el resultado de un ensayo para tres horas de ejecución de la aplicación, en la primera y tercera hora se realizaron movimientos bruscos mientras que en la segunda no.

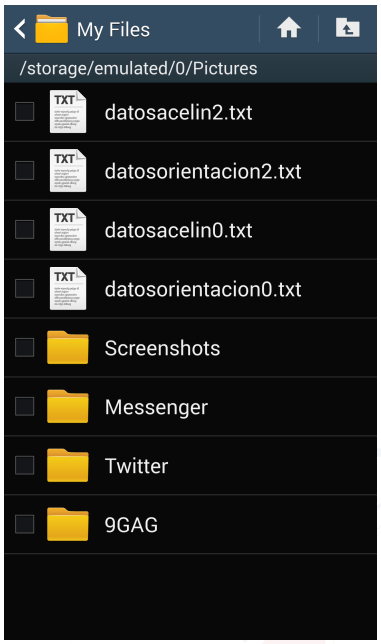


Figura 3.9: Optimización del sistema de almacenamiento.

3.3. Resultados

A partir de varios ensayos y pruebas realizadas se pude afirmar que la aplicación es estable en su ejecución y cumple con todos los parámetros de diseño propuestos. Existen algunos errores de aproximación en cuanto al número de pasos y altura sobre el nivel del mar entregados por la aplicación, lo cual se aprecia de mejor manera al correr la aplicación en diferentes teléfonos inteligentes, sin embargo, es posible obviar dichos errores ya que no representan un problema para los fines posteriores de esta investigación, como la reconstrucción gráfica de la trayectoria que siguió un individuo en la que únicamente se utilizan valores relativos del desplazamiento horizontal y vertical del dispositivo. El resto de datos obtenidos y almacenados no presentan mayor problema en cuanto a su exactitud.

Finalmente, en la implementación de la aplicación se tuvo especial cuidado con respecto a la manipulación de los datos, únicamente redondeando dichos valores a unos cuantos decimales para su adecuado almacenamiento, por lo que la información almacenada esta constituida por mediciones directas de los sensores del teléfono inteligente y puede tomarse como fuente valedera de evidencia digital en caso de la ocurrencia de un siniestro.

Capítulo 4

Procesamiento y análisis de los datos

El procesamiento y análisis de los datos obtenidos por la aplicación móvil se realizó en MATLAB, este IDE integra la computación, programación, procesamiento de señales y gráficos en un mismo entorno, además contiene un sin número de herramientas matemáticas y estadísticas que fueron de gran ayuda para la obtención de los resultados que se presentan a lo largo de esta sección.

La presente sección consta de cuatro etapas secuenciales, las cuales se resumen en la Figura 4.1.

Figura 4.1: Secuencia del procesamiento y análisis de los datos .

4.1. Lectura de los datos

Como se explicó en la sección 3.2, la aplicación móvil guarda los datos obtenidos de los sensores en dos archivos de texto: **"datosacelin0.txt"** y **"datosorientacion0.txt"**, estos archivos contienen la información correspondiente a una hora, por lo que resultan muy extensos para la realización de pruebas de análisis y procesamiento que puedan arrojar resultados contundentes sobre la identificación de movientes brus-

cos. Se optó por la creación de un nuevo método en la aplicación móvil el cual guarda en un archivo 5 pruebas de 10 segundos cada una, se creyó conveniente el tiempo de 10 segundos ya que en este intervalo se obtienen 500 muestras, suficientes para la identificación de características representativas. En los archivos de texto se identifica a cada prueba gracias al carácter especial **"@"** que sirve como separador entre pruebas. Al leer el archivo en MATLAB, la totalidad de los datos se almacenan como un solo vector, lo que complica el acceso individual a los mismos, por esta razón se realiza el procedimiento mostrado en la Figura 4.2.

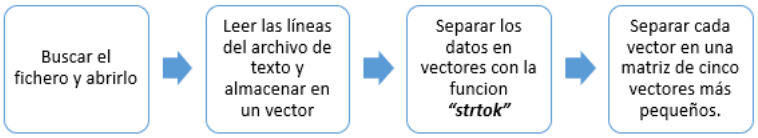


Figura 4.2: Proceso para leer los archivos.

Luengo de realizar el primer y segundo paso de este procedimiento, el resultado obtenido en MATLAB es el que se muestra en la Figura 4.3.

```
'0.0283 -1.3394 0.1859 0 0 18:10:08 2016 02 25'
'0.6943 -1.2447 0.5051 0 0 18:10:08 2016 02 25'
'0.8247 -0.7221 0.4932 0 0 18:10:09 2016 02 25'
'0.5193 -0.6082 -0.3201 0 0 18:10:09 2016 02 25'
'-0.3175 -1.0563 -2.0206 0 0 18:10:09 2016 02 25'
'-1.0280 -0.6156 -3.4612 0 0 18:10:09 2016 02 25'
'-0.5272 -0.1242 -2.4865 0 0 18:10:09 2016 02 25'
'-0.3850 -0.8942 -1.2922 0 0 18:10:09 2016 02 25'
'-0.0311 -0.8818 0.8652 0 0 18:10:09 2016 02 25'
'0.7908 -0.6614 2.9767 0 0 18:10:09 2016 02 25'
'0.9116 -0.5204 1.5612 0 0 18:10:09 2016 02 25'
'@ @ @ @'
'0.4968 -3.4461 -1.8762 0 0 18:10:09 2016 02 25'
'0.3017 -1.6934 -2.9773 0 0 18:10:09 2016 02 25'
'0.4918 0.4221 -0.9127 0 0 18:10:09 2016 02 25'
'0.5527 1.2510 0.6660 0 0 18:10:09 2016 02 25'
'-0.5660 -0.4793 -1.0683 0 0 18:10:09 2016 02 25'
'-1.1406 -1.6745 -4.0788 0 0 18:10:09 2016 02 25'
'-0.6082 -1.5748 -3.5148 0 0 18:10:09 2016 02 25'
'0.7267 -1.1096 -0.6325 0 0 18:10:09 2016 02 25'
```

Figura 4.3: Vector resultante al abrir y leer el archivo "datosacelin0.txt".

Cada elemento de este vector resultante constituye un registro con varios datos, los primeros tres corresponden a las aceleraciones lineales de los tres ejes del teléfono inteligente que serán utilizados para la extracción de características y la implementación del algoritmo de detección. Es por esto que en el tercer paso del procedimiento se

pretende separar los datos en columnas que se almacenan en vectores individuales, para lograr lo anterior se utiliza la función "***strtok***", mediante la cual se detecta el carater espacio.

Una vez separadas las columnas es necesario realizar una subdivisión de las mismas ya que estas almacenan los datos correspondientes a cinco pruebas diferentes, en el cuarto paso lo que se hace es comparar cada elemento de los vectores con el caracter especial **"@"** (véase Figura 4.4) y al encontrar una coincidencia se almacenan todos los datos previos en un nuevo vector, lo anterior se realiza hasta obtener los vectores correspondientes a las cinco pruebas

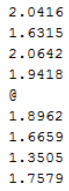


Figura 4.4: Separador entre pruebas.

4.2. Extracción de características principales de los datos

Para poder detectar los movimientos bruscos se procede a obtener un conjunto de características de las cinco pruebas en las que se realizaron diferentes actividades, esto en base a proyectos y trabajos de investigación realizados anteriormente por otros autores [28][34], en los cuales se mencionaba que es posible detectar o identificar actividades como: caminar, correr, estar de pie, etc. Mediante la adquisición de las características de las señales correspondientes a las lecturas del acelerómetro. Las características que se obtuvieron para cada señal fueron:

- Kurtosis
  Ecuación matemática (Ecuación 4.2.1):

$$K = n\frac{\sum_{i=1}^{n}(X_i - X_{avg})^4}{(\sum_{i=1}^{n}(X_i - X_{avg})^2)^2} \tag{4.2.1}$$

  Comando en MATLAB:

  K=kurtosis(X)

- Skewness

Ecuación matemática (Ecuación 4.2.2):

$$S = \sqrt[2]{n}\frac{\sum_{i=1}^{n}(X_i - X_{avg})^3}{(\sum_{i=1}^{n}(X_i - X_{avg})^2)^{3/2}} \tag{4.2.2}$$

Comando en MATLAB:

$$S{=}skewness(X)$$

- Mean
  Ecuación matemática (Ecuación 4.2.3):

$$\mu = \frac{\sum_{i=1}^{n} X_i}{n} \tag{4.2.3}$$

  Comando en MATLAB:

$$\mu = mean(X)$$

- Standard deviation
  Ecuación matemática (Ecuación 4.2.4):

$$\sigma = \sqrt[2]{\frac{\sum_{i=1}^{n}(X_i - \mu)^2}{n}} \tag{4.2.4}$$

  Comando en MATLAB:

$$\sigma = std(X)$$

Y las cinco actividades que se realizaron fueron:

- Subir gradas
- Bajar gradas
- De pie
- Caminar
- Correr

El conjunto de actividades citadas anteriormente, fueron efectuadas cumpliendo dos características principales a) sin efectuar movimientos bruscos para su ejecución y b) efectuando movimientos bruscos, es decir en el primer caso se realizaron las actividades de forma constante sin ningún movimiento inusual y en el segundo caso de igual forma se realizaron las actividades de forma constante pero simulando un movimiento brusco

en cualquier instante de tiempo. Esto con la finalidad de observar si las características varían entre las señales.

A continuación en las Figuras 4.5 y 4.6 se muestran las gráficas de las señales en x, y, z del primer y segundo conjunto de pruebas al realizar las actividades mencionadas sin movimientos bruscos.

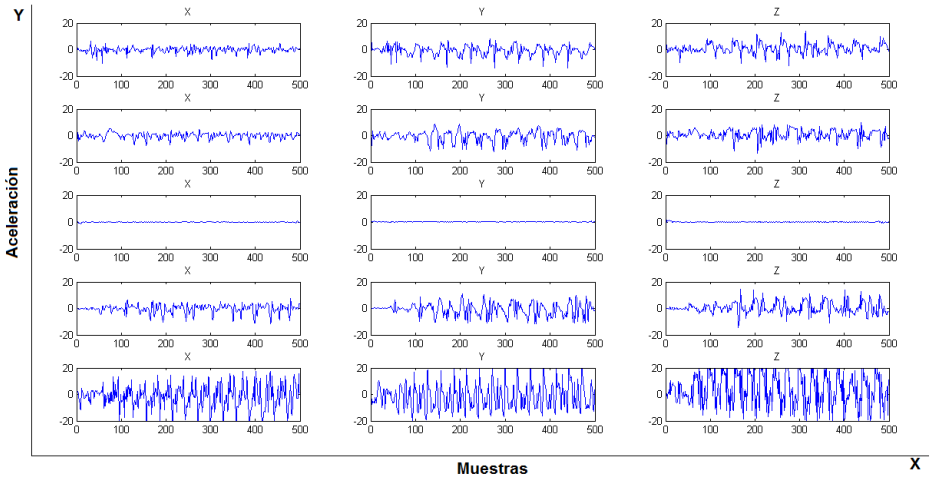


Figura 4.5: Señales de las componentes x, y, z del acelerómetro en la prueba N°1 al realizar las cinco actividades sin movimientos bruscos.

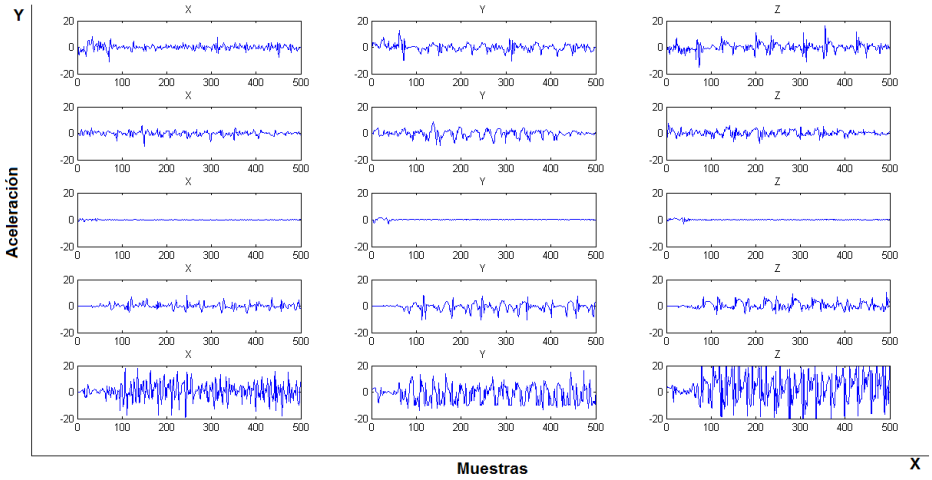


Figura 4.6: Señales de las componentes x, y, z del acelerómetro en la prueba N°2 al realizar las cinco actividades sin movimientos bruscos.

En las Figuras 4.7 y 4.8 se muestran las gráficas de las señales en x, y, z del primer y segundo conjunto de pruebas al realizar las actividades mencionadas con movimientos bruscos.

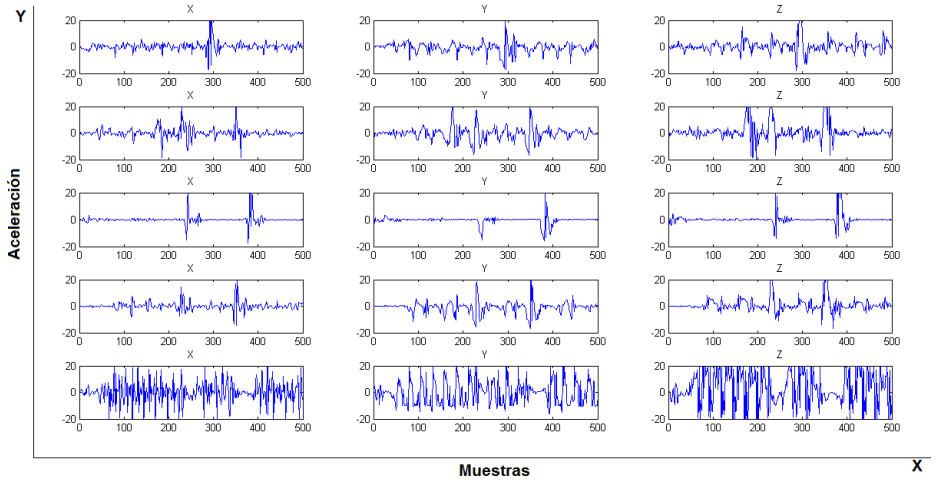


Figura 4.7: Señales de las componentes x, y, z del acelerómetro en la prueba N°1 al realizar las cinco actividades con movimientos bruscos.

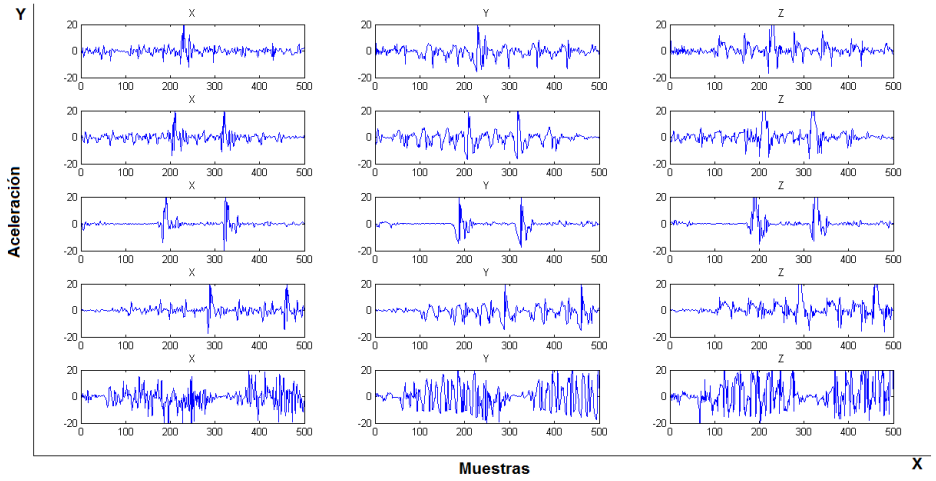


Figura 4.8: Señales de las componentes x, y, z del acelerómetro en la prueba N°2 al realizar las cinco actividades con movimientos bruscos.

En las Tablas 4.1 y 4.2 se muestran los valores de las características obtenidos para las cinco diferentes actividades sin movimientos bruscos para los dos conjuntos de

pruebas, y en las Tablas 4.3 y 4.4 se muestran los valores de las características obtenidos para las cinco diferentes actividades con movimientos bruscos para los dos conjuntos de pruebas. Se adquieren las características para las componentes de aceleración en x, y, z y también para la aceleración resultante.

Características de las señales	Componente x	Componente y	Componente z	Resultante
Subir gradas				
Kurtosis	5.8787	3.9299	0.0035	5.1131
Skewness	-0.8352	-0.6127	0.0035	1.2627
Mean	-0.1605	-0.5552	1.0562	4.7702
Standard deviation	1.9461	3.6706	3.6106	2.9916
Bajar gradas				
Kurtosis	3.7764	3.2026	-0.4564	2.8867
Skewness	-0.6326	-0.6700	-0.4564	0.6447
Mean	-0.0221	-0.3596	0.9457	5.1050
Standard deviation	2.1154	4.0177	3.4214	2.6898
De pie				
Kurtosis	8.3946	8.4742	1.6072	22.8016
Skewness	-0.9174	0.4539	1.6072	3.5660
Mean	-0.0729	0.0968	0.0134	0.2935
Standard deviation	0.2112	0.1282	0.2357	0.2125
Caminar				
Kurtosis	4.7560	2.7730	0.3311	2.2240
Skewness	-1.1341	-0.1991	0.3311	0.4756
Mean	-0.2583	-0.5715	0.6770	5.9800
Standard deviation	3.1217	4.5804	4.2752	3.7448
Correr				
Kurtosis	3.5008	2.7407	-0.0642	2.8104
Skewness	-0.4001	0.4769	-0.0642	0.4839
Mean	-1.7794	-1.7911	4.2334	15.9029
Standard deviation	8.2188	9.3206	11.7149	7.9118

Tabla 4.1: Valores de las características obtenidos al realizar las cinco actividades sin movimientos bruscos en la Prueba N°1.

Características de las señales	Componente x	Componente y	Componente z	Resultante
Subir gradas				
Kurtosis	6.7049	5.7884	0.1734	8.4691
Skewness	-0.2260	0.0781	0.1734	1.9565
Mean	0.0801	0.0461	0.0984	3.6466
Standard deviation	1.9383	2.6023	3.0471	2.5510
Bajar gradas				
Kurtosis	6.8589	3.9603	-0.0353	4.7048
Skewness	-0.8560	-0.6099	-0.0353	1.1740
Mean	-0.0377	-0.0298	0.3208	3.1432
Standard deviation	1.5862	2.5965	2.0229	1.8856
De pie				
Kurtosis	21.6596	28.1477	-2.2491	25.0108
Skewness	-1.8194	-2.1704	-2.2491	4.1609
Mean	-0.0889	0.0616	0.0235	0.3378
Standard deviation	0.2588	0.3553	0.3119	0.4341
Caminar				
Kurtosis	4.9323	4.9490	0.4883	3.8775
Skewness	0.4339	-0.6621	0.4883	1.0147
Mean	0.0901	-0.4030	0.6897	3.4388
Standard deviation	1.8164	2.7565	2.5974	2.5381
Correr				
Kurtosis	3.9270	2.1543	-0.0725	2.8107
Skewness	-0.1959	0.0845	-0.0725	0.5936
Mean	0.7538	-1.5281	3.2545	11.9895
Standard deviation	5.8488	6.2458	10.0334	6.5859

Tabla 4.2: Valores de las características obtenidos al realizar las cinco actividades sin movimientos bruscos en la Prueba N°2.

Características de las señales	Componente x	Componente y	Componente z	Resultante
Subir gradas				
Kurtosis	23.5111	8.2945	1.8481	23.1919
Skewness	2.3126	-0.3085	1.8481	3.9362
Mean	0.3691	-0.4856	0.7244	5.0253
Standard deviation	3.4609	3.9326	4.7886	5.0958
Bajar gradas				
Kurtosis	15.0739	6.3604	1.5922	9.3919
Skewness	0.8286	0.3007	1.5922	2.4468
Mean	0.1021	-0.4526	1.1858	5.9535
Standard deviation	3.6392	5.0795	6.1857	6.5891
De pie				
Kurtosis	33.8115	20.2659	3.9205	23.1775
Skewness	3.0673	-1.9491	3.9205	4.3892
Mean	0.0724	-0.4570	0.2863	2.1424
Standard deviation	2.8769	2.7611	4.0198	5.2685
Caminar				
Kurtosis	16.1689	7.9477	2.6445	14.3987
Skewness	1.7294	0.0981	2.6445	3.0681
Mean	0.1457	-0.8169	1.0198	4.8020
Standard deviation	3.0506	4.3583	5.2922	5.9106
Correr				
Kurtosis	4.3838	2.5283	-0.0217	2.1770
Skewness	-0.2173	0.4926	-0.0217	0.2651
Mean	-0.0176	-0.3697	3.1021	15.1227
Standard deviation	7.4931	8.8391	12.5873	8.5640

Tabla 4.3: Valores de las características obtenidos al realizar las cinco actividades con movimientos bruscos en la Prueba N°1.

Características de las señales	Componente x	Componente y	Componente z	Resultante
Subir gradas				
Kurtosis	18.5659	6.9671	1.7551	16.2780
Skewness	1.5572	-0.1569	1.7551	3.0614
Mean	0.0754	-0.4848	0.9553	4.9914
Standard deviation	2.6840	4.1947	4.6680	4.7730
Bajar gradas				
Kurtosis	14.9817	6.0067	2.2062	13.2243
Skewness	1.6941	-0.1141	2.2062	2.8974
Mean	0.0281	-0.5432	0.7901	5.5531
Standard deviation	3.4482	4.7218	5.4663	5.8386
De pie				
Kurtosis	22.9332	15.2586	3.3935	15.9347
Skewness	1.6458	-0.5441	3.3935	3.5262
Mean	0.0847	-0.4404	0.5327	3.0445
Standard deviation	3.2127	3.3778	4.8243	6.0170
Caminar				
Kurtosis	12.4902	6.2133	1.8468	11.8753
Skewness	1.1624	0.0941	1.8468	2.6360
Mean	0.2511	-0.9389	1.1469	5.6536
Standard deviation	3.5858	4.4544	5.6059	5.8619
Correr				
Kurtosis	5.2463	2.7291	0.4924	2.9450
Skewness	-0.2438	0.1637	0.4924	0.6795
Mean	-0.7040	-0.0269	2.2683	11.8450
Standard deviation	6.2089	8.5319	9.6686	8.3603

Tabla 4.4: Valores de las características obtenidos al realizar las cinco actividades con movimientos bruscos en la Prueba N°2.

Como se puede observar en las tablas, no se puede establecer un patrón general a partir de los valores obtenidos para caracterizar a las señales con o sin movimientos bruscos, esto se debe a que existe una diferencia notable en los valores según el tipo de actividad realizada. En otras palabras, estas características no representan un argumento valedero para poder detectar la existencia de actividad motriz inusual sin importar el tipo de actividad realizada, que es el tema que nos compete en la presente sección. Los resultados anteriores podrían ser de utilidad si se buscara la identificación del tipo de actividad realizada ya que se podría establecer un rango de convergencia a partir de la realización de varias pruebas y utilizarlo en el desarrollo de un algoritmo de clasificación, sin embargo, este tema esta fuera del alcance de este trabajo.

4.3. Diseño e implementación del algoritmo de detección

Dado que los resultados obtenidos en la sección 4.2 no son de ayuda para la detección de actividad motriz inusual, se optó por seguir un camino distinto. En primer lugar se observó, en las gráficas obtenidas para las componentes x, y, z, que existen ciertos picos, positivos o negativos, que son producto de la realización de movimientos bruscos sin importar la actividad ejecutada, esto se puede apreciar en la Figura 4.7 y en la Figura 4.8 del anterior apartado. Además, teniendo en cuenta que la realización de actividad inusual se puede ver reflejada en cualquiera de los tres ejes del acelerómetro, ya sea distribuyéndose entre estos o manifestándose en uno solo, se determinó que sería factible llevar a cabo la detección a partir de los valores obtenidos para la aceleración resultante definida por la ecuación (3.2.1). Al trabajar con la aceleración resultante es posible resumir en una sola magnitud el comportamiento de las tres componentes sin importar el signo de éstas. Lo anterior se pude visualizar de mejor manera en la Figura 4.9, en la que existen dos picos mucho más grandes que los picos en las componentes x, y, z.

Después de realizar varias pruebas de las actividades con movimientos bruscos, se pudo definir un valor umbral para la aceleración resultante mediante el cual el algoritmo sea capaz de establecer si existió un movimiento brusco o no. Por ejemplo, al observar las gráficas de las resultantes de un conjunto de pruebas (véase Figura 4.10), se puede apreciar que los picos correspondientes a los movimientos bruscos sobrepasan el valor de 20 m/s^2, por lo que se definió este valor como referencia para la detección. Es decir, si un valor de la aceleración resultante es mayor a 20 m/s^2 se puede afirmar que fue generado por un movimiento brusco. Este valor umbral de la aceleración resultante es muy útil ya que no solo se utiliza en este algoritmo como parámetro principal para la

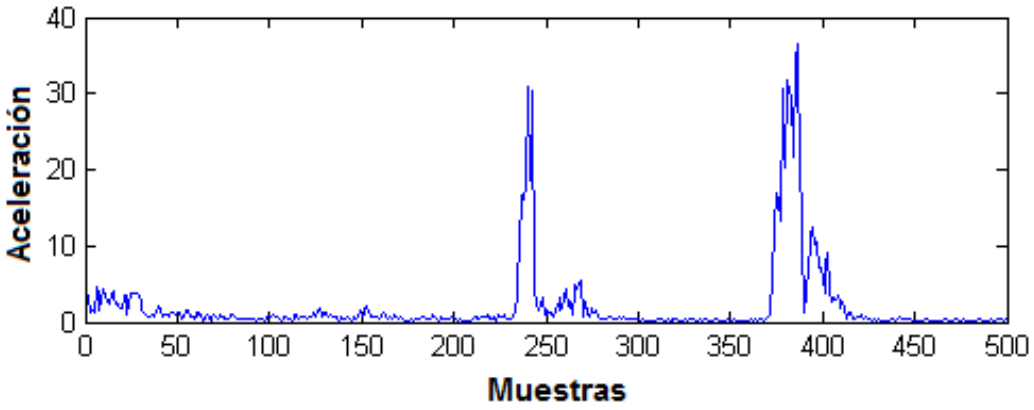


Figura 4.9: Gráfica de la resultante al realizar la actividad de pie con movimientos bruscos en la Prueba N°1.

detección, sino que también cumple un rol importante en el procesamiento en tiempo real de la aplicación móvil para poder activar el GPS.

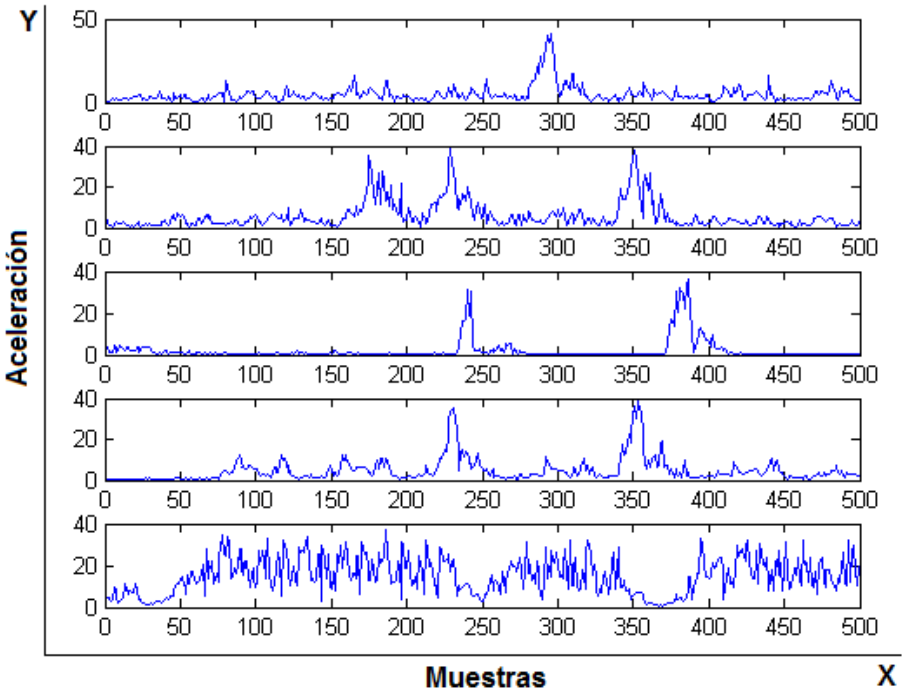


Figura 4.10: Gráfica de las resultantes al realizar las actividades con movimientos bruscos en la Prueba N°1.

Esta solución parece no ser aplicable a todas las actividades que se realizaron en las pruebas ya que al ejecutarse la actividad de correr con movimientos bruscos, existen muchos valores en la resultante que son mayores a 20 m/s^2 como se puede apreciar en la Figura 4.11. Estos valores se dan no solo por movimientos bruscos sino que también son producidos por los rápidos movimientos del cuerpo en general de la posible víctima, lo que ocasiona un problema para el algoritmo de detección ya que no se puede diferenciar cuando existió un movimiento brusco o simplemente fue la actividad de correr.

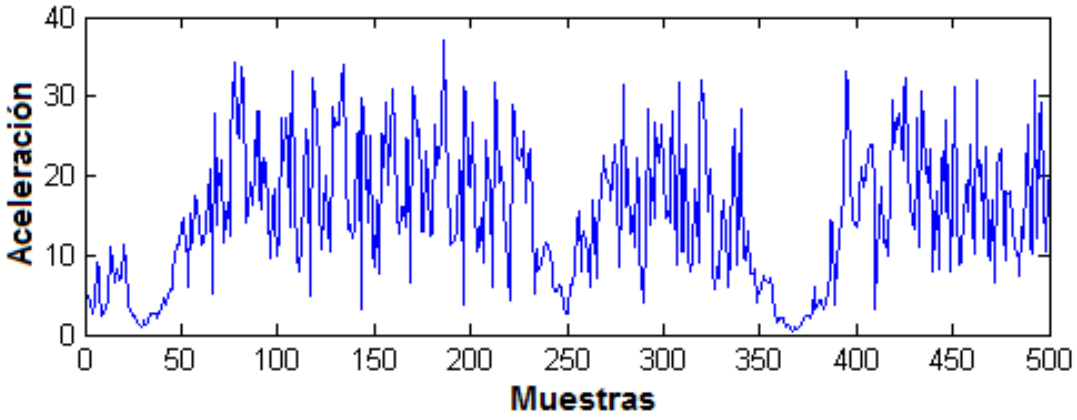


Figura 4.11: Gráfica de la resultante al realizar la actividad de correr con movimientos bruscos en la Prueba N°1.

Debido a este problema, adicionalmente al valor umbral se planteó otra condición para poder diferenciar un movimiento brusco al momento de realizar actividades similares a las de correr en las que existen varios valores de la resultante mayores a 20 m/s^2. La única diferencia entre la realización de un movimiento brusco y un movimiento repetitivo como el correr, es que después de un movimiento brusco existe un gran número de muestras que son menores a 20 m/s^2 como se puede observar en la Figura 4.12, donde existen más de 50 valores que están por debajo de la linea roja es decir que son menores a 20 m/s^2, con esta característica particular de la señal de la aceleración resultante se pudo finalmente implementar un algoritmo que pueda distinguir un movimiento brusco de cualquier otro tipo de actividad o movimiento.

El algoritmo implementado trabaja a partir del vector que contiene los valores de las aceleraciones resultantes calculadas para cada prueba, y su diagrama de flujo se muestra en la Figura 4.13.

A continuación se explica de manera general los pasos seguidos por el algoritmo:

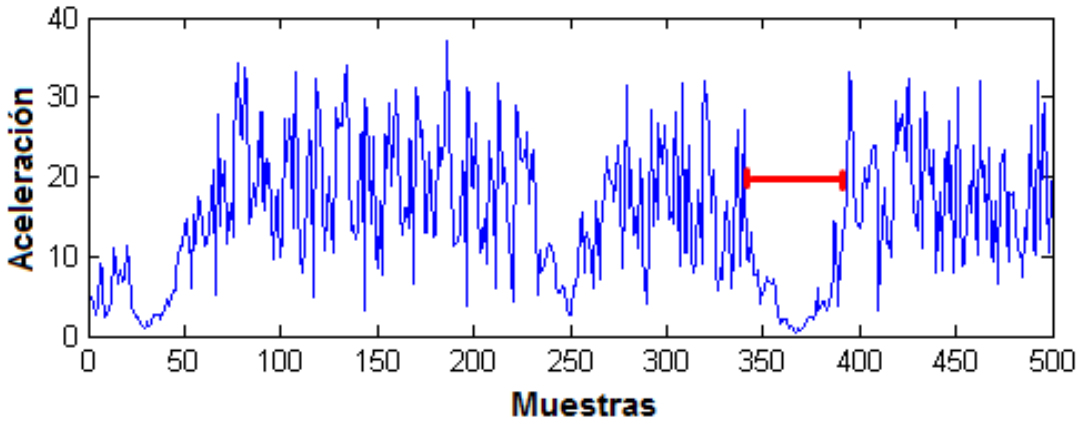


Figura 4.12: Detección de un movimiento brusco al realizar la actividad de correr en la Prueba N°1.

1. Lee un dato del vector de las aceleraciones resultantes.
2. Verifica si el dato es mayor a 20, si lo es, almacena la posición del dato y hace cero el contador de valores menores a 20. En caso de no ser mayor a 20, verifica si existió por lo menos un dato mayor a 20 almacenado previamente, si existió algún dato, el contador de valores menores a 20 aumenta una unidad; en caso de no existir el algoritmo termina para el dato actual.
3. Verifica si el contador de datos menores a 20 es mayor a 50, es decir, que luego de un dato mayor a 20 existieron por lo menos 50 datos menores a 20 de forma consecutiva. En caso de ser así se almacena la posición del dato como un movimiento brusco, caso contrario el algoritmo termina para el dato actual.
4. Notifica el movimiento brusco y se muestra en que posición existió dicho movimiento.
5. Finaliza el algoritmo para el dato actual.
6. Realiza este procedimiento para todos los datos del vector hasta llegar a la última posición en donde finaliza completamente el algoritmo.

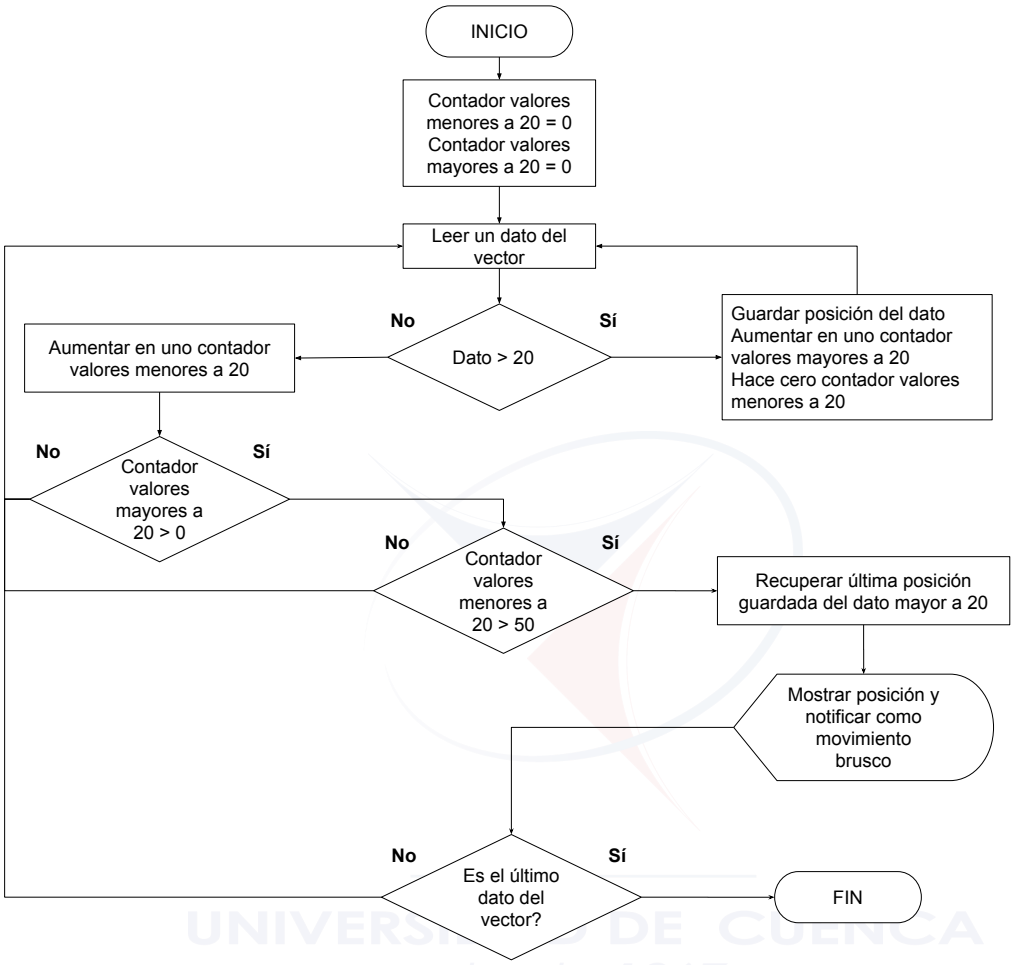


Figura 4.13: Algoritmo de detección de movimientos bruscos.

4.4. Pruebas de rendimiento y precisión

Ya con el algoritmo implementado, este se aplica al conjunto de pruebas de las cinco actividades realizadas sin movimientos bruscos y con movimientos bruscos. Los resultados obtenidos fueron los siguientes: Para las aceleraciones resultantes de las cinco actividades sin movimientos bruscos en la prueba N°1 (véase Figura 4.14) se obtuvo un total de 0 movimientos bruscos al aplicar el algoritmo de identificación como se describe en la Tabla 4.5.

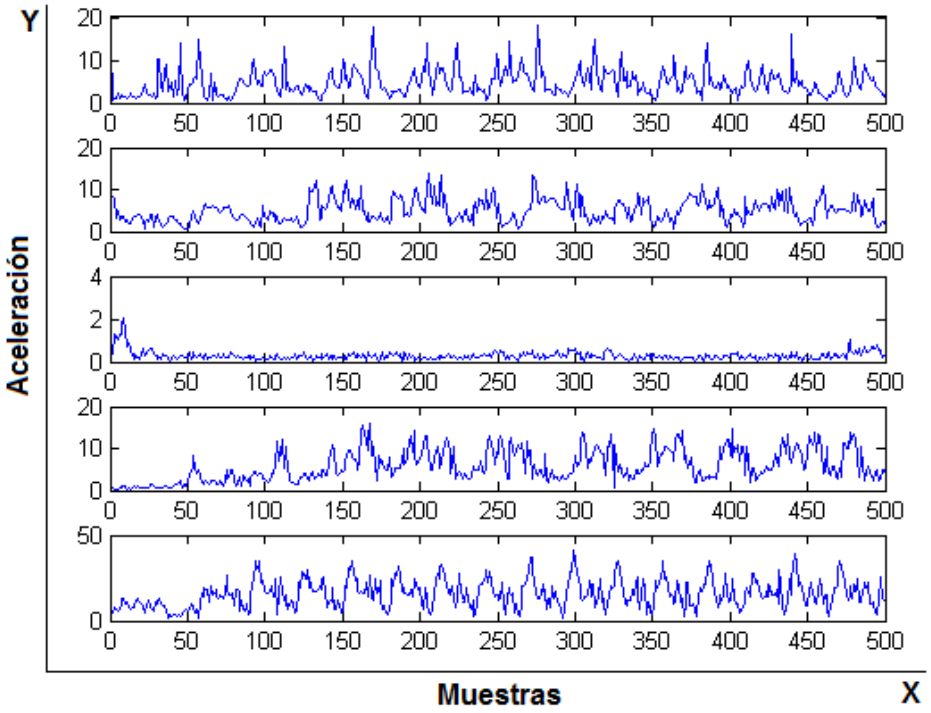


Figura 4.14: Gráfica de las resultantes al realizar las actividades sin movimientos bruscos en la Prueba N°1.

Actividades realizadas	**Cantidad de movimientos bruscos**
Subir gradas	0
Bajar gradas	0
De pie	0
Caminar	0
Correr	0
Total	0

Tabla 4.5: Cantidad de movimientos bruscos en Prueba N°1 al realizar las actividades sin movimientos bruscos.

Para las aceleraciones resultantes de las cinco actividades sin movimientos bruscos en la prueba N°2 (véase Figura 4.15) se obtuvo un total de 0 movimientos bruscos al aplicar el algoritmo de identificación como se describe en la Tabla 4.6.

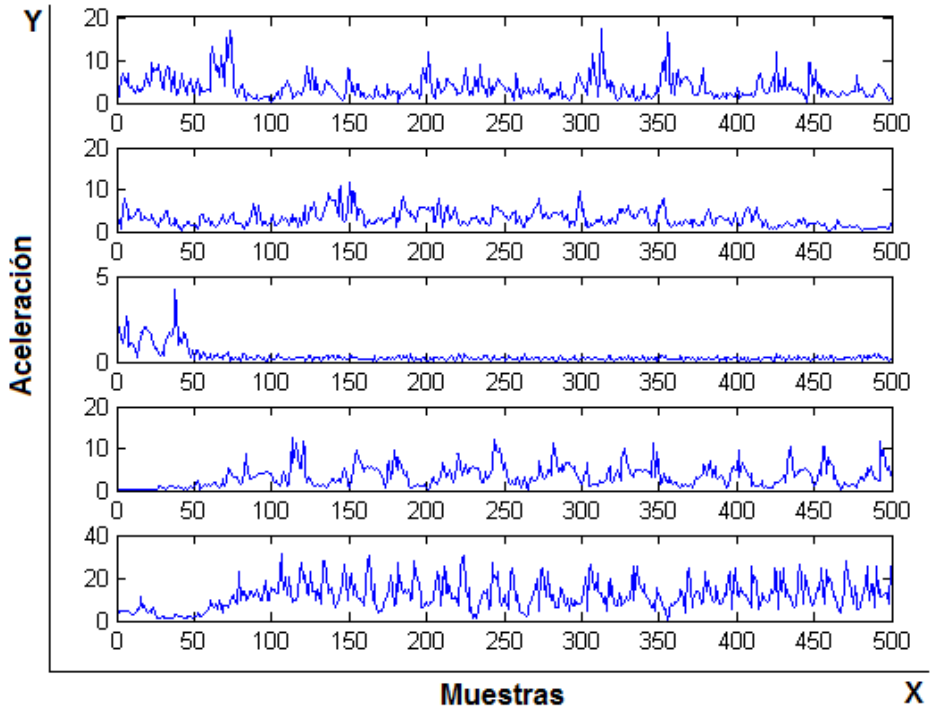


Figura 4.15: Gráfica de las resultantes al realizar las actividades sin movimientos bruscos en la Prueba N°2.

Actividades realizadas	Cantidad de movimientos bruscos
Subir gradas	0
Bajar gradas	0
De pie	0
Caminar	0
Correr	0
Total	0

Tabla 4.6: Cantidad de movimientos bruscos en Prueba N°2 al realizar las actividades sin movimientos bruscos.

Para las aceleraciones resultantes de las cinco actividades con movimientos bruscos en la prueba N°1 (véase Figura 4.16) se obtuvo un total de 8 movimientos bruscos al aplicar el algoritmo de identificación como se describe en la Tabla 4.7.

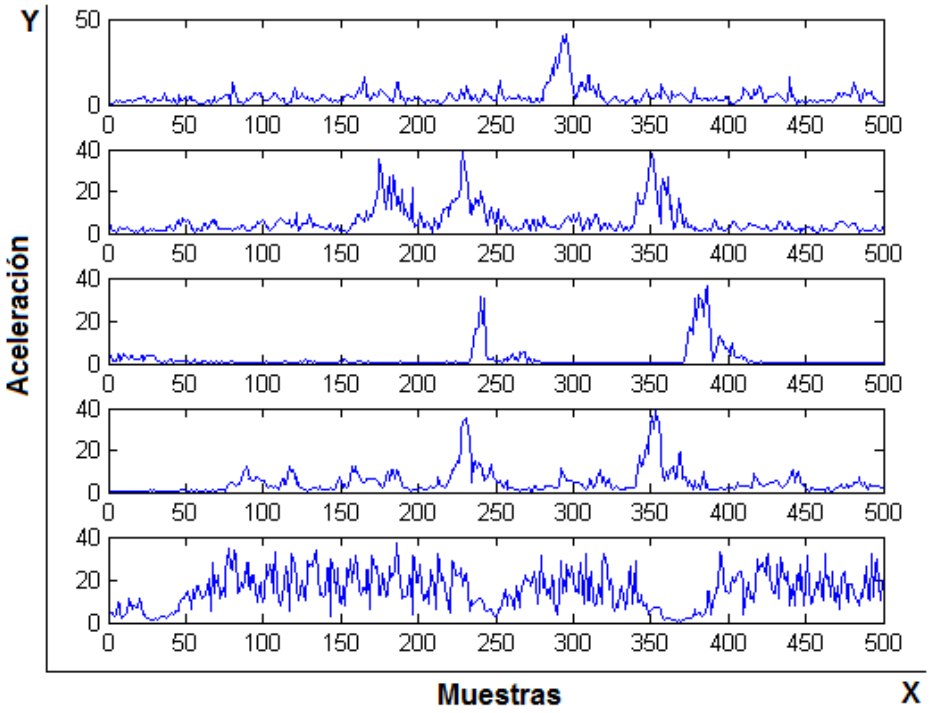


Figura 4.16: Gráfica de las resultantes al realizar las actividades con movimientos bruscos en la Prueba N°1.

Actividades realizadas	**Cantidad de movimientos bruscos**
Subir gradas	1
Bajar gradas	2
De pie	2
Caminar	2
Correr	1
Total	8

Tabla 4.7: Cantidad de movimientos bruscos en Prueba N°1 al realizar las actividades con movimientos bruscos.

Para las aceleraciones resultantes de las cinco actividades con movimientos bruscos en la prueba N°2 (véase Figura 4.17) se obtuvo un total de 8 movimientos bruscos al aplicar el algoritmo de identificación como se describe en la Tabla 4.8.

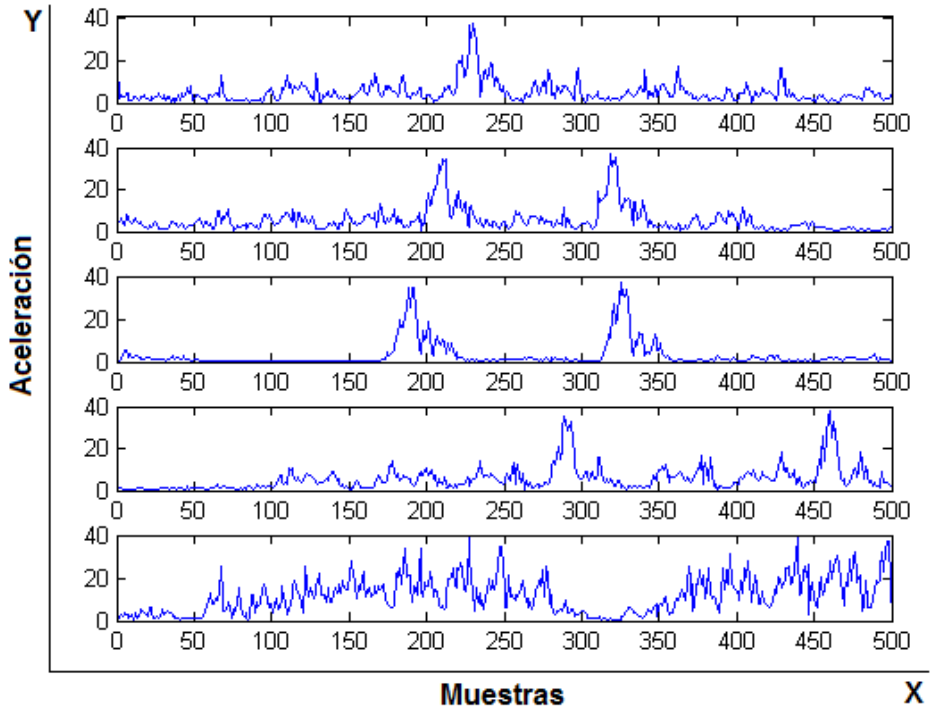


Figura 4.17: Gráfica de las resultantes al realizar las actividades sin movimientos bruscos en la Prueba N°2.

Actividades realizadas	Cantidad de movimientos bruscos
Subir gradas	1
Bajar gradas	2
De pie	2
Caminar	1
Correr	2
Total	8

Tabla 4.8: Cantidad de movimientos bruscos en Prueba N°2 al realizar las actividades con movimientos bruscos.

Finalmente se realiza una comparación entre la cantidad de movimientos bruscos detectados por el algoritmo y la cantidad de movimientos bruscos realizados en las pruebas estableciendo así la precisión del algoritmo.

Actividades realizadas	Movimientos bruscos Calculados		Movimientos bruscos Práctica	
	Prueba N°1	**Prueba N°2**	**Prueba N°1**	**Prueba N°2**
Subir gradas	0	0	0	0
Bajar Gradas	0	0	0	0
De pie	0	0	0	0
Caminar	0	0	0	0
Correr	0	0	0	0
Total	**0**	**0**	**0**	**0**

Tabla 4.9: Cantidad de movimientos bruscos calculados vs. real al realizar las actividades sin movimientos bruscos.

Como se puede observar en la Tabla 4.9, existe la misma cantidad de movimientos bruscos detectados por el algoritmo y realizados en la práctica. Entonces se puede decir que el algoritmo tiene un valor del 100 % de precisión cuando se aplica en actividades sin movimientos bruscos.

Actividades realizadas	Movimientos bruscos Calculados		Movimientos bruscos Práctica	
	Prueba N°1	**Prueba N°2**	**Prueba N°1**	**Prueba N°2**
Subir gradas	1	1	1	1
Bajar Gradas	2	2	2	2
De pie	2	2	2	2
Caminar	2	1	2	1
Correr	1	2	1	1
Total	**8**	**8**	**8**	**7**

Tabla 4.10: Cantidad de movimientos bruscos calculados vs. real al realizar las actividades con movimientos bruscos.

Como se puede observar en la Tabla 4.10, no existe la misma cantidad de movimientos bruscos calculados por el algoritmo y realizados en la práctica. Entonces se puede afirmar que el algoritmo no tiene un valor del 100 % de precisión cuando se aplica en actividades con movimientos bruscos. Para las pruebas realizadas se obtuvo una precisión del 92.85 %. Este valor no siempre es el mismo, dependerá de los tipos de movimientos o actividades que se realicen ya que pueden existir actividades en las que al aplicarlas el algoritmo puedan reflejar movimientos bruscos aunque en la práctica no existan.

Capítulo 5

Aplicación de escritorio para la recreación gráfica de eventos

La aplicación de escritorio fue creada en MATLAB con el propósito de brindar al investigador forense un ambiente amigable mediante el cual se pueda realizar una navegación temporal de los eventos registrados como bruscos o inusuales. A partir de la misma se puede analizar la trayectoria seguida por la víctima en los instantes de interés de forma visual en tres dimensiones, también consta de herramientas de visualización para la ubicación en un mapa global del sitio del suceso y de la aceleración resultante de los tramos de tiempo seleccionados.

5.1. Diseño e implementación del algoritmo de recreación

El algoritmo trabaja a partir de un conjunto de datos los cuales se resumen en la Tabla 5.1. Todos estos datos se obtienen de los dos archivos generados por la aplicación móvil.

Datos
Ángulo (Azimuth)
Altura
Componentes x, y, z del acelerómetro

Tabla 5.1: Datos necesarios para la implementación del algoritmo de recreación.

El diagrama de flujo del algoritmo se puede observar en la Figura 5.1.

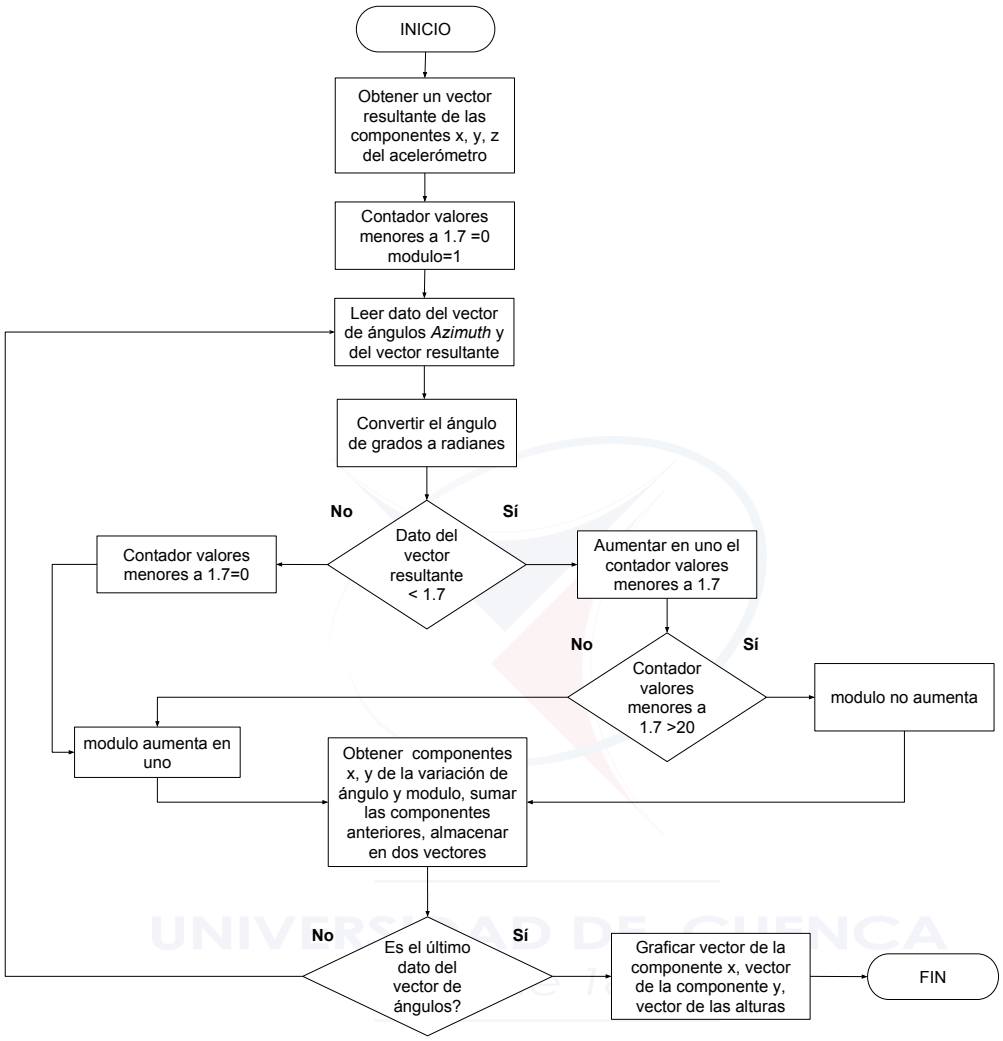


Figura 5.1: Algoritmo de recreación.

A continuación se explica de manera general los pasos seguidos por el algoritmo:

1. Obtiene un vector cuyos elementos corresponden a las aceleraciones resultantes, esto con la finalidad de posteriormente comprobar si la víctima no tuvo movimiento alguno, es decir, si se mantuvo fija en un lugar. Para lo cual se comparará con el valor de 1.7 ya que al estar el teléfono sin movimiento todos los datos de la aceleración resultante son menores a dicho valor.
2. Convierte de grados a radianes un dato del vector de ángulos utilizando la ecua-

ción 5.1.1.

$$vectradianes(i) = \frac{vectgrados(i) * \pi}{180} \tag{5.1.1}$$

3. Verifica si un dato del vector de las aceleraciones resultantes (misma posición que el dato del vector de ángulos) es menor a 1.7, si el dato no lo es la variable modulo aumenta una unidad. Si el dato lo es el contador de valores menores a 1.7 aumenta una unidad y luego verifica si dicho contador es mayor a 20, si lo es la variable modulo no aumenta, en cambio si el contador no es mayor a 20 entonces la variable modulo aumenta una unidad. Todo esto se lo realiza para comprobar si la persona estuvo o no en movimiento.
4. Obtiene las componentes x, y de la variación de ángulo y la variación de modulo, y sumar el valor anterior de las componentes x, y, utilizando la ecuación 5.1.2 y la ecuación 5.1.3 respectivamente.

$$componentesx(i) = componentesx(i-1) + ((modulo(i+1) - modulo(i)) * cos(vectradianes(i+1) - vectradianes(i))) \tag{5.1.2}$$

$$componentesy(i) = componentesy(i-1) + ((modulo(i+1) - modulo(i)) * sin(vectradianes(i+1) - vectradianes(i))) \tag{5.1.3}$$

5. Almacena las componentes x, y en dos vectores.
6. Si finalizaron todos los datos del vector de ángulos graficar en tres dimensiones el vector de altura, el vector de la componente x y el vector de la componente y, caso contrario seguir con el próximo dato del vector de ángulos.
7. Si finalizaron todos los datos del vector de ángulos el algoritmo termina.

5.2. Funcionamiento general

Como se explicó en secciones previas de la presente investigación, la aplicación móvil realiza la creación de varios archivos, uno por cada hora, con el objetivo de optimizar el sistema de almacenamiento descartando aquellos archivos correspondientes a horas en los que no se registró actividad motriz inusual. Por lo tanto, la aplicación de escritorio, fue diseñada e implementada de tal forma que permita el análisis de la actividad motriz de una víctima una hora a la vez.

En la Figura 5.2 se muestra la interfaz gráfica de la aplicación de escritorio en ejecución:

Figura 5.2: Interfaz gráfica principal de la aplicación de escritorio.

En la sección **Selección de archivos** se incluyen dos botones para la selección de los dos archivos que contienen la información recogida de los diferentes sensores del teléfono móvil durante una hora específica, al pulsar cada uno de estos botones se muestra un explorador de archivos que facilita la selección y la obtención de la ruta de cada archivo. La selección de archivos constituye el primer paso para la correcta ejecución de la aplicación y se puede realizar en cualquier momento (véase Figura 5.3).

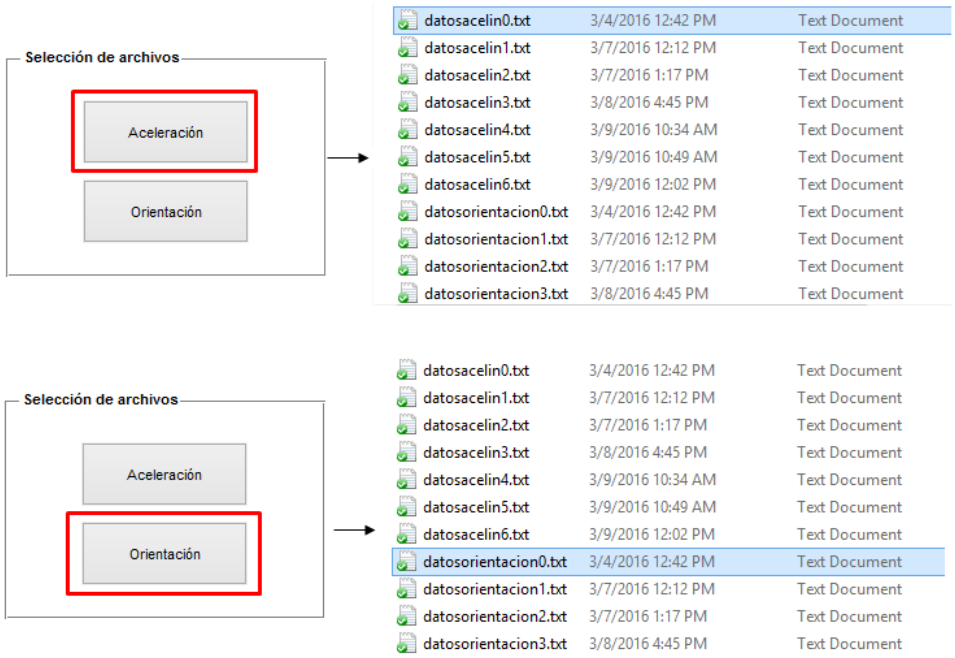


Figura 5.3: Selección de archivos.

En el panel **Cargar movimientos bruscos**, un botón ejecuta el mismo algoritmo de detección diseñado e implementado en la sección 4.3, los resultados se muestran como una lista de fechas y horas de ocurrencia correspondientes a los eventos de actividad inusual detectados en la hora de análisis. A partir de esta lista se puede realizar una navegación en el tiempo y al seleccionar un ítem de la misma, la aplicación muestra en detalle la información referente a las coordenadas geográficas del SS (véase Figura 5.4).

En el siguiente panel de la interfaz gráfica, denominado **Aceleración resultante**, existen varios elementos, uno de ellos y el más grande, es un **axes** que permite la visualización de la aceleración resultante con respecto al número de muestras durante un intervalo definido de tiempo. Este intervalo es tanto para muestras anteriores así como para muestras posteriores, con centro en el número de muestra en el que ocurrió el movimiento brusco, es así que, si se seleccionó un intervalo correspondiente a 500

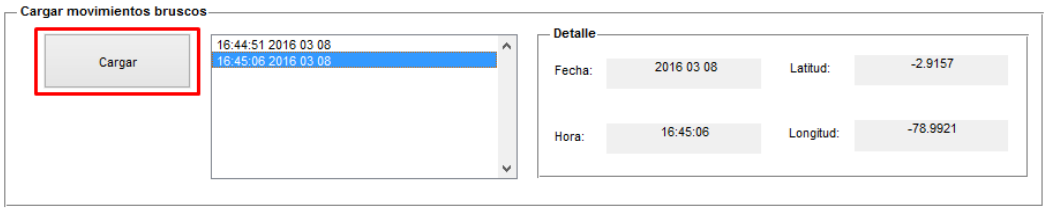


Figura 5.4: Cargar movimientos bruscos.

muestras, la aplicación graficará la aceleración resultante correspondiente a 500 muestras anteriores y posteriores a la muestra de ocurrencia. Mediante el botón **OK** se puede actualizar el número de muestras a graficarse, así como obtener la equivalencia total en segundos del intervalo introducido. Al pulsar el botón **Graficar Todo** se ignora el intervalo introducido por el usuario y se toman todas las muestras obtenidas en los 3600 segundos correspondientes a la hora de análisis para el gráfico de la aceleración resultante. Se consideró necesaria la visualización de la aceleración resultante dentro de la interfaz de la aplicación ya que a partir de ésta se puede tener una noción del tipo de actividad realizada por la víctima al momento de la detección de un movimiento brusco. En esta sección también se muestra el número total de pasos dados por la víctima, y en función a esta magnitud se calcula la cantidad total de metros recorridos, en este último computo se tomó como equivalencia que un paso sea igual 0.8 metros (véase Figura 5.5).

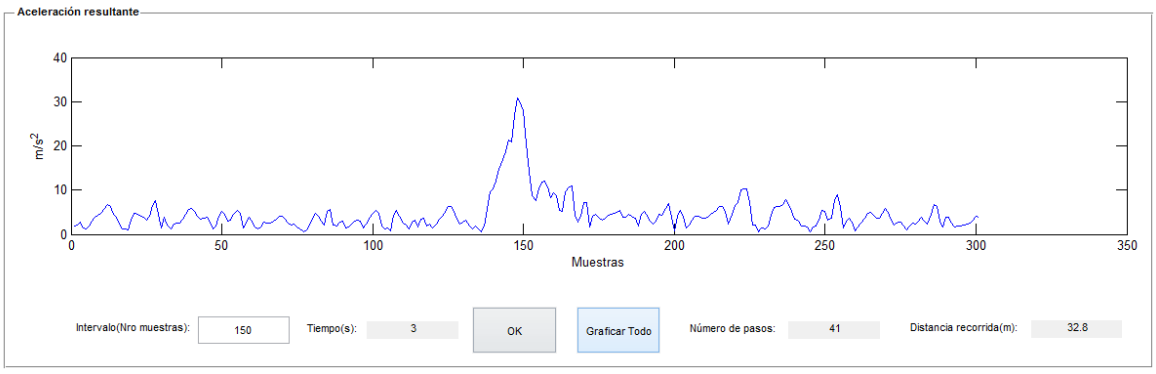


Figura 5.5: Gráfico de la aceleración resultante.

La función del botón **Simulación 3D**, ubicado en la sección lateral derecha de la interfaz (véase Figura 5.2), es la de mostrar dos nuevas interfaces en las cuales se grafica

la trayectoria de la víctima en tres dimensiones según el intervalo de muestras y tiempo previamente elegido.

En la primera interfaz se realiza una recreación animada en la que un círculo traza la trayectoria desde el inicio hasta el final del intervalo, mediante el botón **Refrescar** se puede apreciar nuevamente la animación. Esta animación es importante ya que otorga al usuario un mayor grado de comprensión sobre los desplazamientos dados por la víctima al momento del incidente (véase Figura 5.6).

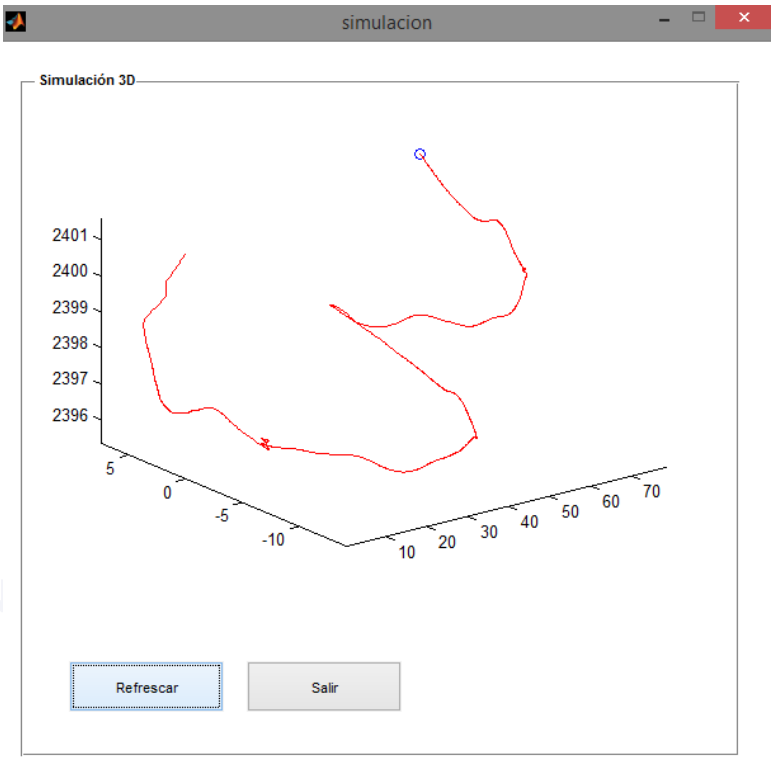


Figura 5.6: Animación de la trayectoria en tres dimensiones.

En la segunda interfaz únicamente se grafica la trayectoria sin ningún tipo de animación pero se agregan herramientas que permiten la rotación, acercamiento y alejamiento de la gráfica. Mediante estas herramientas es posible apreciar la trayectoria desde varios ángulos y planos, además se señalan los puntos de ocurrencia de movimientos bruscos mediante círculos rojos (véase Figura 5.7).

Por último, el botón **Geolocalización** ubicado en la misma sección que el botón **Simulación 3D** (véase Figura 5.2), permite ubicar en un mapa global el lugar en el que ocurrió el siniestro mediante el uso del archivo **plot_google_map.m** creado por

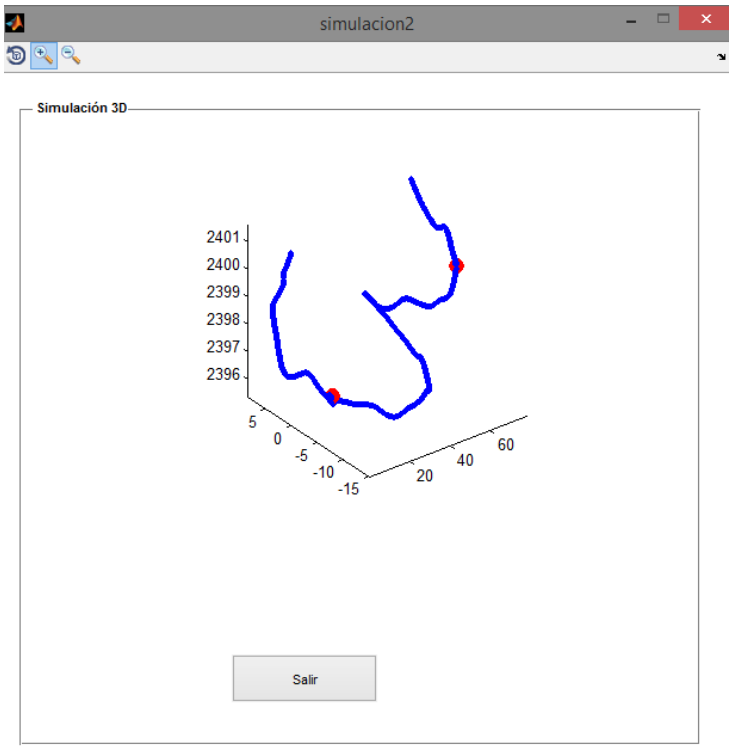


Figura 5.7: Gráfico de la trayectoria en tres dimensiones.

Zohar Bar-Yehuda y obtenido en [39], página oficial de MATLAB para el intercambio de archivos entre la comunidad de usuarios del software. Este archivo toma como parámetros de entrada únicamente la latitud y longitud del punto en formato decimal, y presenta los resultados en una nueva interfaz como se muestra en la Figura 5.8.

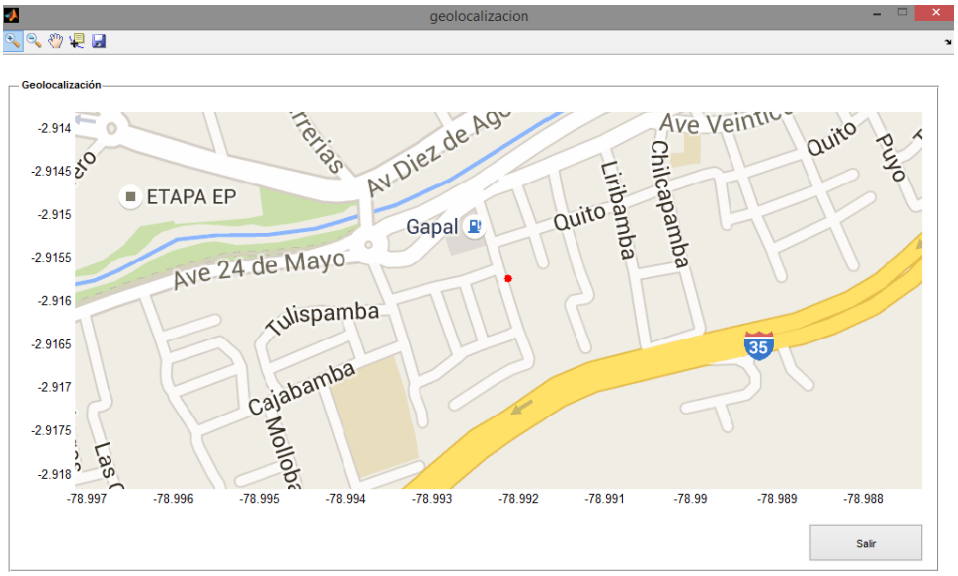


Figura 5.8: Geolocalización a partir de las coordenadas del SS.

5.3. Resultados

Con la finalidad de comprobar el correcto funcionamiento de la aplicación se realizaron varias pruebas de campo en diferentes lugares. A continuación se muestran cuatro pruebas realizadas en lugares con diferente arquitectura y elevaciones para poder comprobar que el algoritmo de recreación y la aplicación funcionan de manera correcta. Cabe recalcar que las pruebas se realizaron con el teléfono móvil en la mano así como también colocado en uno de los bolsillos delanteros del pantalón de la víctima, lugares en donde comúnmente se mantiene el teléfono inteligente.

En la Figura 5.9 se puede observar unas escaleras que tienen una forma particular la cuales pertenecen a una edificación de la Universidad de Cuenca, se denota el inicio de la trayectoria con la letra “I” y el final con la letra “F”, la recreación de la trayectoria realizada en dicho lugar se puede apreciar en la Figura 5.10.

Figura 5.9: Gráfico del sitio de la trayectoria de la prueba N°1.

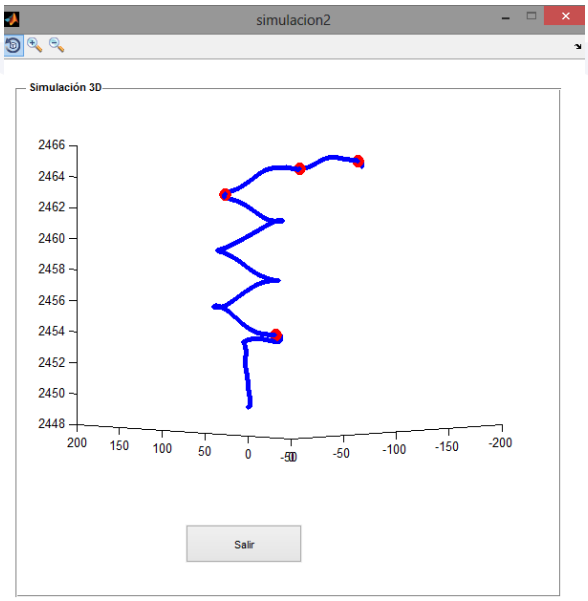


Figura 5.10: Gráfico de la reconstrucción de la trayectoria de la prueba N°1.

En la Figura 5.11 se puede observar una locación de la Universidad de Cuenca entre la Facultad de Ingeniera y la de Arquitectura, se denota el inicio de la trayectoria con la letra “I” y el final con la letra “F”, la recreación de la trayectoria realizada en dicho lugar se puede apreciar en la Figura 5.12.

Figura 5.11: Gráfico del sitio de la trayectoria de la prueba N°2.

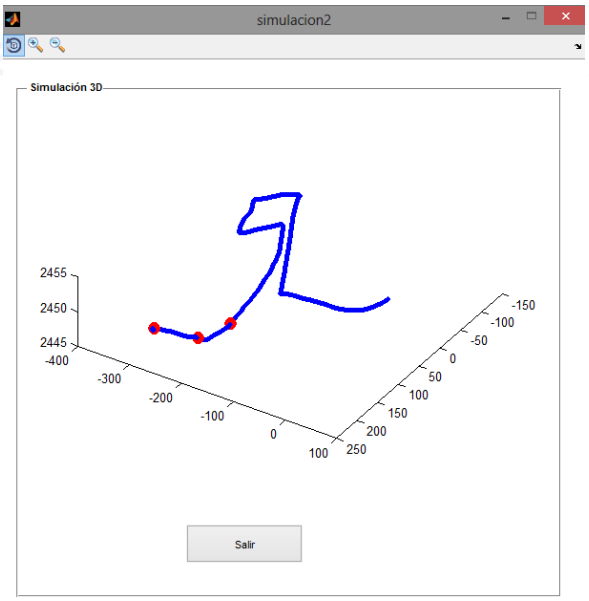


Figura 5.12: Gráfico de la reconstrucción de la trayectoria de la prueba N°2.

En la Figura 5.13 se puede observar otra locación de la Universidad de Cuenca entre la biblioteca hasta la puerta lateral de la Facultad de Arquitectura, se denota el inicio de la trayectoria con la letra “I” y el final con la letra “F”, la recreación de la trayectoria realizada en dicho lugar se puede apreciar en la Figura 5.14.

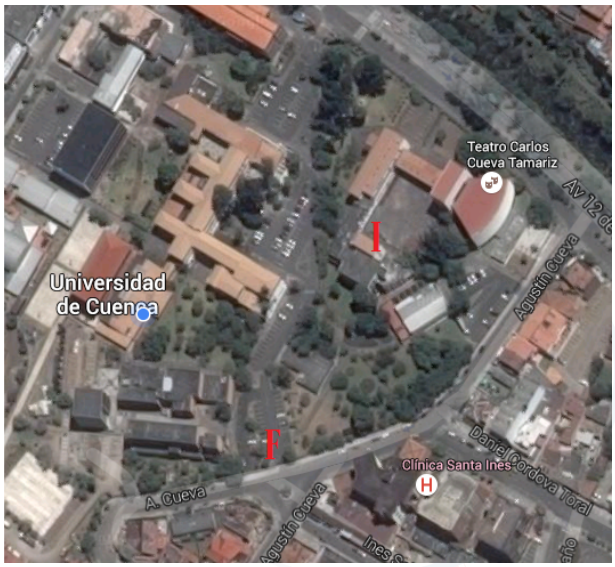


Figura 5.13: Gráfico del sitio de la trayectoria de la prueba N°3.

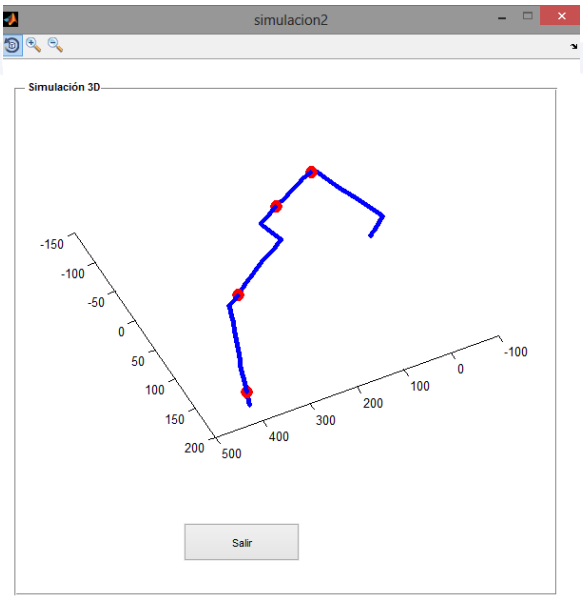


Figura 5.14: Gráfico de la reconstrucción de la trayectoria de la prueba N°3.

En la Figura 5.15 se puede observar la combinación de unas escaleras en el interior de una edificación con un patio el cual tiene un montículo o elevación notable, se denota el inicio de la trayectoria con la letra “I” y el final con la letra “F”, la recreación de la trayectoria realizada en dicha combinación de lugares se puede apreciar en la Figura 5.16.

Figura 5.15: Gráfico del sitio de la trayectoria de la prueba N°4.

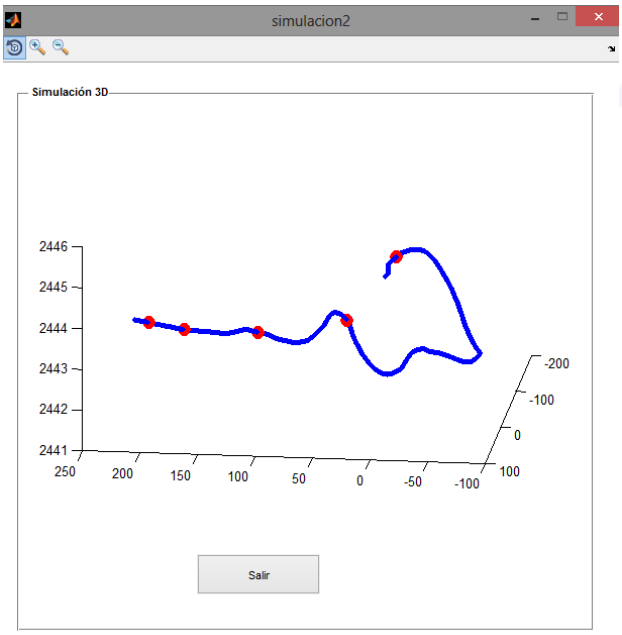


Figura 5.16: Gráfico de la reconstrucción de la trayectoria de la prueba N°4.

Como se puede observar en las cuatro pruebas de campo realizadas en lugares con distintas arquitecturas y elevaciones, los resultados obtenidos son satisfactorios ya que las trayectorias recreadas en tres dimensiones se asemejan de gran manera a las trayectorias realizadas en la práctica. Puede existir pequeñas variaciones en la altura y en los ángulos de las trayectorias, lo cual no afecta significativamente en la recreación ni a los propósitos de esta investigación que buscan dar una noción acertada a los investigadores periciales sobre la actividad motriz de una posible víctima.

Capítulo 6

Conclusiones y Recomendaciones

6.1. Conclusiones

Luego de lo expuesto a lo largo de las diferentes secciones que forman parte de la presente investigación, se puede afirmar que uno de los ejes principales de la misma constituye la adquisición de datos de un teléfono inteligente. Estos dispositivos cuentan con una gran cantidad de sensores y métodos relacionados a los mismos que son capaces de proporcionar variada información, convirtiéndolos en potenciales fuentes de evidencia digital. El seleccionar adecuadamente los sensores según las necesidades y objetivos del trabajo, representa un parte crucial de la investigación, y gracias a esto fue posible desarrollar herramientas y obtener resultados de gran relevancia para el análisis digital forense.

Con el fin de detectar actividad motriz inusual o movimientos bruscos se optó por la utilización de la información proveniente del acelerómetro del teléfono inteligente, sin embargo, debido a la presencia de la gravedad de la Tierra y su influencia en las mediciones, se estableció que no solo es necesario obtener las aceleraciones registradas en los tres ejes del dispositivo sino que estas deben ser aceleraciones lineales, es decir aquellas en las que se anula por completo la gravedad. El uso de aceleraciones que no son del tipo lineal genera en el algoritmo de detección resultados erróneos ya que este, buscando lograr su objetivo de la forma más precisa posible, utiliza como principal parámetro a la aceleración resultante, cantidad que se ve afectada por la magnitud de la gravedad que se distribuye en los tres ejes del dispositivo según su posición de no anularse su efecto.

Uno de los aspectos importantes del algoritmo de detección de movimientos bruscos, es que logra cumplir su cometido sin importar el tipo de activad que haya estado reali-

zando la víctima cuando ocurrió un incidente. Por ejemplo, se demostró que a pesar de que la víctima permanece estática, caminando, corriendo, subiendo o bajando escaleras, se logra la detección de manera exitosa. Esto se debe a que la aceleración resultante, además de resumir en una sola magnitud las tres componentes referentes a los ejes del teléfono inteligente, constituye una medida característica del movimiento de la víctima y más aún ante la ocurrencia de actividad inusual. Se intento extraer características de las tres señales de aceleraciones lineales obtenidas mediante el cálculo de otras medidas matemáticas y estadísticas con el fin de robustecer al algoritmo, pero se determinó que los resultados no eran contundentes ya que no demostraban la ocurrencia de algún movimiento inusual, justificándose así, la utilización de la aceleración resultante como único parámetro para la detección.

En cuanto al algoritmo para la recreación gráfica de la trayectoria de la víctima en tres dimensiones, se puede decir que los resultados obtenidos cuentan con un alto grado de exactitud y precisión. En primera instancia se pensaba utilizar los mismos datos de las aceleraciones lineales de los tres ejes del dispositivo para la obtención de desplazamientos mediante una doble integración, sin embargo, y luego de una minuciosa indagación sobre el tema, se decidió que este no era el camino a tomar debido al error que puede generar una integración numérica en los resultados. También se omitió el uso del GPS con el objetivo de evitar recreaciones erróneas en ambientes del tipo *indoor*. Finalmente la solución recayó nuevamente en la adquisición de datos del teléfono inteligente, esta vez se optó por la extracción de información angular referente a la orientación del dispositivo además de su altura con respecto al nivel del mar obteniéndose resultados positivos en la implementación del algoritmo con estos datos.

Se tuvo especial cuidado al momento de extraer información referente a la geolocalización de la víctima, restringiendo la adquisición de coordenadas del GPS únicamente ante la detección de eventos inusuales. Este fue un tema de importancia al momento de implementar la aplicación Android con el fin de evitar una violación a la privacidad de la víctima. También se hizo énfasis en la optimización del sistema de almacenamiento ya que toda la información recopilada de los sensores se guarda en archivos de texto y a pesar de que su tamaño individual es relativamente pequeño, luego de un uso prolongado de la aplicación, se puede generar una sobrecarga en la memoria interna del dispositivo. Dicha optimización consiste principalmente en la creación de nuevos archivos por cada hora de uso de la aplicación, de esta forma al finalizar este periodo de tiempo, la aplicación tiene la capacidad de eliminar aquellos archivos en los que no se registró ningún tipo de actividad motriz inusual por parte de la víctima.

Finalmente es necesario acotar que algunos de los datos extraídos del teléfono inte-

ligente no son del todo exactos, por ejemplo se pudo apreciar que al correr la aplicación móvil en distintos dispositivos, en un mismo lugar, se obtenían lecturas distintas en cuanto a la altura sobre el nivel del mar. También existen ocasiones en que los datos provistos por el GPS tienen un pequeño error cuando el dispositivo se encuentra en ambientes del tipo *indoor*. Por último, se detectaron falencias en el contador de pasos utilizado en esta investigación, una de éstas es que se tarda en entregar los primeros resultados al momento de ejecutar por primera vez la aplicación y en unas pocas ocasiones no se detectó correctamente el instante en el que se da un paso.

A criterio de los investigadores, cada una de las herramientas desarrolladas en la presente investigación pudieran ser utilizadas de manera exitosa en investigaciones relacionadas al análisis digital forense. La extracción de datos a partir de los sensores de un teléfono inteligente mediante la aplicación desarrollada, cumple con el principio de fiabilidad ya que se evitó la manipulación de la información por parte del software dado que únicamente realiza procesos de obtención y almacenamiento de datos en el dispositivo. Además, la aplicación de escritorio ofrece varias herramientas que facilitan el entendimiento de los hechos ocurridos en el SS en base a los datos obtenidos, estas herramientas permiten la visualización y animación de la trayectoria seguida por la víctima en tres dimensiones, ubicación en un mapa global de las coordenadas del sitio en el que ocurrió el siniestro y la determinación de la distancia total recorrida por la víctima. Se puede decir que la aplicación móvil y la aplicación de escritorio, utilizadas en conjunto, constituyen un recurso valedero para lograr la resolución de un caso.

6.2. Recomendaciones

Al momento de instalar la aplicación en un teléfono inteligente con el sistema operativo Android se debe tomar en cuenta la versión del sistema ya que la aplicación móvil esta diseñada para ejecutarse correctamente desde la versión 4.0.3 (Ice Cream Sandwich MR1) en adelante. No se garantiza el correcto desempeño de todas las funcionalidades de la aplicación móvil desarrollada en versiones anteriores a la mencionada.

Otro de los aspectos a tomarse en cuenta tiene que ver con la aplicación de escritorio, esta fue implementada en MATLAB en su versión R2013b por lo que su ejecución y el correcto funcionamiento del software pueden verse afectados en versiones más antiguas del IDE.

6.3. Trabajos Futuros

A futuro se pretende desarrollar la aplicación móvil para otros sistemas operativos como iOS y Windows Phone dado que existe un número considerable de teléfonos inteligentes que no cuentan con el sistema operativo Android. También se tiene previsto la publicación de la aplicación móvil en las respectivas tiendas de los tres sistemas operativos, garantizando así, el acceso a la misma.

Capítulo 7

Anexos

7.1. Anexo 1

Análisis digital forense de los sensores de un teléfono inteligente para la detección y recreación de actividad motriz inusual en una localización determinada

David Espinoza Farfán, david.espinozaf@ucuenca.ec,
Juan Martín Yánez Rodas, juan.yanezr@ucuenca.ec, Mgst. Karina Campos Argudo, karinacampos@ucuenca.edu.ec

***abstract*—The objective of this research is to develop a new methodology in order to detect and recreate unusual motor activity from a possible victim in a determined location. This work is framed within the field of digital forensic analysis, branch of criminology which is in charge of obtaining potential digital evidence from electronic devices with criminal purposes by applying a set of adequate techniques and procedures.**

This work has as its base the use of information obtained from a smartphone, so in first instance an application for the Android operative system is developed with the purpose of extracting and registering measurements from some sensors of the device. Once the information is stored it is processed and analyzed in MATLAB, from which the identification of abrupt movements is achieved regardless of the type of activity performed by the victim at the time of the incident. Finally, a desktop application is developed in the same platform, it contains a graphical interface in which is presented the digitalized reconstruction in three dimensions of the trajectory followed by the victim, as well as the geographic location of the exact site where the incident occurred. In the desktop application is also presented other information relevant to the forensic research like the resultant acceleration before and after the occurrence of unusual activity, the date and hour, number of steps taken by the victim and the total distance of displacement.

***Keywords*—digital forensics analysis, digital evidence, sensors, accelerometer, unusual activity, graphic recreation.**

I. Introducción

El análisis o peritaje digital constituye una de las ramas de más reciente auge dentro del ámbito forense, sin embargo, es una de las disciplinas con mayor potencial ya que mediante este tipo de investigación es posible extraer información de un siniestro que de otra forma sería muy difícil o imposible. Hoy en día, distintos dispositivos electrónicos, en especial los teléfonos inteligentes, constituyen una fuente valedera de evidencia, que puede ser utilizada en un juicio si se realiza de manera correcta el peritaje respectivo con el fin de obtener e interpretar la información que estos son capaces de proporcionar. Dentro del análisis digital forense la mayoría de metodologías tiene como objetivo adquirir evidencias relacionadas con la interacción de la víctima y sus dispositivos electrónicos dentro del campo enteramente digital, es decir, se enfocan principalmente en la extracción de archivos, registros, historiales, etc. Que pudieran relacionarse con las circunstancias del siniestro.

En esta investigación se propone una nueva metodología, que se enfoca en la extracción de la información referente a la actividad motriz de la víctima, es decir, se basa en el mismo principio básico de anteriores técnicas de obtener información digital de los dispositivos pero de fuentes distintas como son los sensores con los que cuentan los teléfonos inteligentes. Varios de estos sensores pueden entregar información referente al movimiento de la víctima en cualquier instante, y de hecho se han utilizado para la creación de aplicaciones de ocio o relacionadas con el ejercicio físico, pero nunca antes se habían utilizado estos recursos para la detección de actividad motriz inusual.

A continuación se presenta el proceso de adquisición de datos a partir de la creación de una aplicación móvil, los algoritmos de detección y recreación gráfica de actividad inusual, y por último la aplicación de escritorio en la que se muestran los resultados finales del análisis digital forense realizado.

II. Aplicación móvil para la adquisición de eventos

La aplicación desarrollada esta destinada para el funcionamiento en teléfonos inteligentes que cuentan con el sistema operativo Android, y se implementó enteramente en Android Studio que es el IDE oficial para el desarrollo de aplicaciones Android. La aplicación recopila información sobre el dispositivo como su aceleración, ubicación geográfica, orientación, conteo de pasos, altitud, hora y fecha. A partir de toda esta información es posible realizar la detección de actividad motriz inusual así como la reconstrucción gráfica de los hechos en el sitio del suceso. La interfaz gráfica de la aplicación en funcionamiento se presenta en la Figura 1. Resulta conveniente acotar que, aunque se presentan varias de las lecturas de los sensores en la interfaz gráfica, existen otros datos de gran importancia como la latitud y longitud de la ubicación geográfica obtenidos del GPS, que no se muestran pero que igualmente son almacenados para su posterior procesamiento y análisis. El mostrar en pantalla varios de los datos obtenidos, tiene como única finalidad, otorgar a los investigadores un medio visual para la comprensión adecuada del funcionamiento de los sensores y métodos utilizados en la aplicación.

Fig. 1: Interfaz gráfica de la aplicación desarrollada.

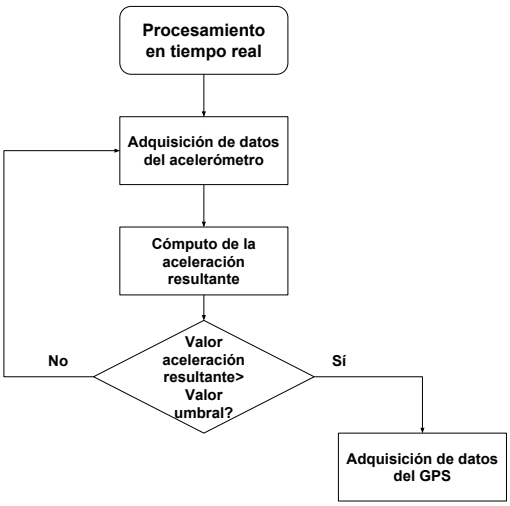


Fig. 2: Procesamiento para la adquisición de datos del GPS.

Para el caso de la detección de actividad motriz inusual está claro que únicamente se requiere adquirir y almacenar los datos del acelerómetro, sin embargo, es necesario llevar a cabo un procesamiento de estos en tiempo real, es decir, en el mismo teléfono inteligente cuando la aplicación se encuentra en ejecución. Lo anterior tiene que ver con la adquisición de información proveniente del GPS del dispositivo, esta información no puede ser registrada de forma continua ya que constituye una violación a la privacidad de la víctima, es así que se ha restringido su almacenamiento unicamente para cuando se producen lecturas del acelerómetro que indican la realización de algún tipo de actividad abrupta.

La forma en la que se determina la ocurrencia de actividad inusual es mediante la comparación de los datos del acelerómetro, específicamente la aceleración resultante, con un valor umbral. Se puede observar en detalle los pasos del procesamiento en tiempo real en el diagrama de flujo de la Figura 2. Los datos del GPS son de considerable importancia ya que mediante estos se puede ubicar a la víctima y al sitio del suceso.

La aceleración resultante se define como la raíz cuadrada de la suma de los cuadrados de las componentes de la aceleración, y matemáticamente se expresa como se muestra en la ecuación (1).

$$a_r = \sqrt{a_x^2 + a_y^2 + a_z^2} \tag{1}$$

La aplicación realiza este cálculo constantemente, y unicamente obtiene los datos del GPS si la aceleración resultante calculada es mayor o igual a 20 m/s^2. Mas adelante se justifica el uso de este valor como parámetro de comparación, pero se puede adelantar que en general la aceleración resultante de un movimiento inusual, es siempre mayor o igual a esta magnitud.

Con respecto a la reconstrucción gráfica de los hechos, y dado que dicha recreación se llevara a cabo en tres dimensiones, resulta indispensable obtener información acerca de la orientación del dispositivo y su desplazamiento tanto horizontal como vertical (véase Figura 3).

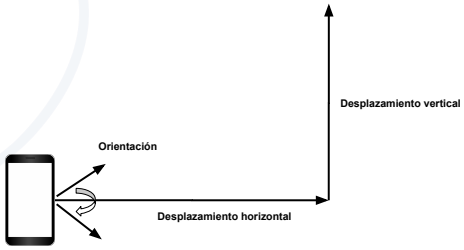


Fig. 3: Datos necesarios para la recreación gráfica.

Finalmente es necesario registrar cada una de las lecturas junto con la fecha y hora en los que se llevó a cabo la adquisición en el teléfono inteligente con el objetivo de ubicar temporalmente la ocurrencia de cualquier tipo de actividad motriz inusual. Todos estos datos deben ser almacenados continuamente por la aplicación a intervalos de tiempo constantes a excepción de los datos del GPS por las razones indicadas anteriormente. Se decidió que la forma más efectiva para el almacenamiento de este conjunto de información es mediante dos archivos de texto localizados en la memoria interna del teléfono inteligente.

El constante almacenamiento de este conjunto de información en archivos de texto por periodos de tiempo prolongados, supone un constante incremento en la utilización de la memoria interna del dispositivo, por lo que es necesario optimizar el uso de la memoria disponible descartando aquellos periodos de tiempo en los que no se detectó algún tipo de actividad motriz inusual. Se estableció que el periodo de tiempo para el almacenamiento sea de una hora, luego de transcurrido este tiempo se comprobará si existió algún tipo de actividad inusual,

si el resultado es afirmativo se conservarán los dos archivos, caso contrario la aplicación procederá con la eliminación de los mismos. Este proceso de optimización se representa mediante un diagrama de flujo en la Figura 4.

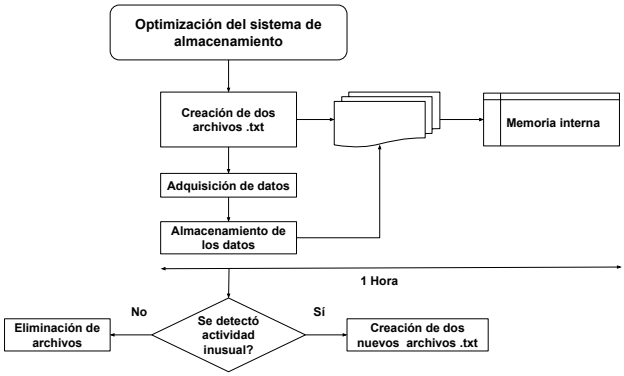


Fig. 4: Optimización del sistema de almacenamiento.

Estos dos archivos son creados en la carpeta ***Pictures*** del dispositivo con los nombres **"datosacelin0.txt**" y **"datosorientacion0.txt**" en las primeras etapas de ejecución de la aplicación. Se decidió diferenciar a los archivos mediante números, razón por la cual se aprecia el número 0 en los nombres de los primeros archivos (véase Figura 5).

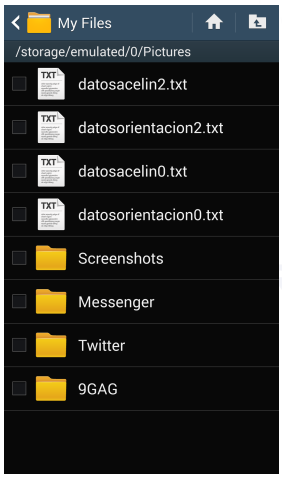


Fig. 5: Archivos creados y eliminados por la aplicación.

En el sistema operativo Android existen varios tipos de sensores [1], en la Tabla I se resumen los utilizados por la aplicación desarrollada.

III. Aplicación de escritorio para la detección y recreación gráfica de eventos inusuales

La aplicación de escritorio fue creada en MATLAB con el propósito de brindar al investigador forense un ambiente amigable mediante el cual se pueda realizar una navegación

Función	Sensor
Acelerómetro	*TYPE_LINEAR_ACCELERATION*
Orientación	*TYPE_ORIENTATION*
Contador de pasos	*TYPE_STEP_COUNTER*
Altímetro	*TYPE_PRESSURE*

Tabla I. Tipos de sensores utilizados y su función.

temporal de los eventos registrados como bruscos o inusuales. A partir de la misma se puede analizar la trayectoria seguida por la víctima en los instantes de interés de forma visual en tres dimensiones, también consta de herramientas de visualización para la ubicación en un mapa global del sitio del suceso y de la aceleración resultante de los tramos de tiempo seleccionados.

A. *Diseño e implementación del algoritmo de detección*

Se realizaron varias pruebas obteniendo valores de cuatro características diferentes en actividades como subir gradas, bajar gradas, estar de pie, caminar y correr. Las características obtenidas fueron las siguientes: kurtosis, skewness, mean y standard deviation. Se pudo apreciar que no es posible establecer un patrón general a partir de dichos valores para caracterizar a las señales con o sin movimientos bruscos, esto se debe a que existe una diferencia notable en los valores según el tipo de actividad realizada. En otras palabras, estas características no representan un argumento valedero para poder detectar la existencia de actividad motriz inusual sin importar el tipo de actividad realizada. Dado que los resultados obtenidos al realizar las pruebas mencionadas anteriormente no son de ayuda para la detección de actividad motriz inusual, se optó por seguir un camino distinto. Se observó en las gráficas obtenidas para las componentes x, y, z, del acelerómetro, que existen ciertos picos, positivos o negativos, que son producto de la realización de movimientos bruscos sin importar la actividad ejecutada, esto se puede apreciar en la Figura 6.

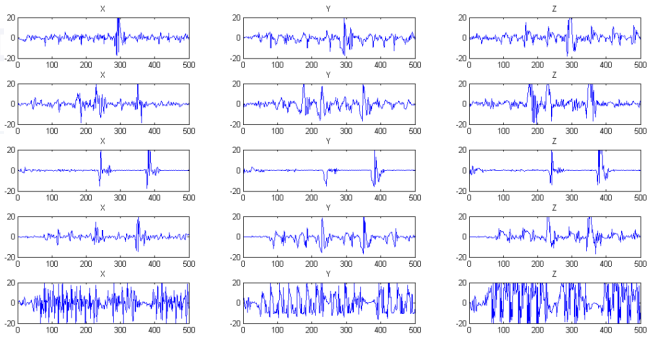


Fig. 6: Señales de las componentes x, y, z del acelerómetro al realizar las actividades de subir gradas, bajar gradas, estar de pie, caminar y correr, con movimientos bruscos.

Además, teniendo en cuenta que la realización de actividad inusual se puede ver reflejada en cualquiera de los tres ejes del acelerómetro, ya sea distribuyéndose entre estos o manifestándose en uno solo, se determinó que sería factible llevar

a cabo la detección a partir de los valores obtenidos para la aceleración resultante definida por la ecuación 1.

Al trabajar con la aceleración resultante es posible resumir en una sola magnitud el comportamiento de las tres componentes sin importar el signo de estas. Lo anterior se pude visualizar de mejor manera en la Figura 7, en la que existen dos picos mucho más grandes que los picos en las componentes x, y, z de la tercera prueba de la Figura 6.

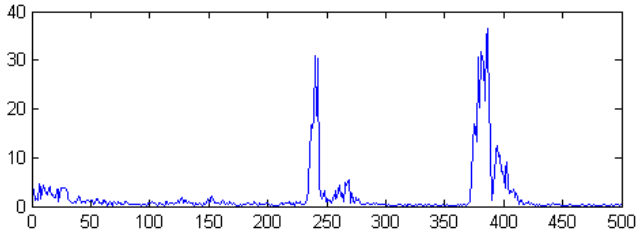


Fig. 7: Gráfica de la resultante al realizar la actividad de pie con movimientos bruscos.

Después de realizar varias pruebas de las actividades con movimientos bruscos, se pudo definir un valor umbral para la aceleración resultante mediante el cual el algoritmo sea capaz de establecer si existió un movimiento brusco o no. Por ejemplo, al observar las gráficas de las resultantes de un conjunto de pruebas (véase Figura 8), se puede apreciar que los picos correspondientes a los movimientos bruscos sobrepasan el valor de 20 m/s^2, por lo que se definió este valor como referencia para la detección. Es decir, si un valor de la aceleración resultante es mayor a 20 m/s^2 se puede afirmar que fue generado por un movimiento brusco. Este valor umbral de la aceleración resultante es muy útil ya que no solo se utiliza en este algoritmo como parámetro principal para la detección, sino que también cumple un rol importante en el procesamiento en tiempo real de la aplicación móvil para poder activar el GPS.

Esta solución parece no ser aplicable a todas las actividades que se realizaron en las pruebas ya que al ejecutarse la actividad de correr con movimientos bruscos, existen muchos valores en la resultante que son mayores a 20 m/s^2 como se puede apreciar en la Figura 9. Estos valores se dan no solo por movimientos bruscos sino que también son producidos por los rápidos movimientos del cuerpo en general de la posible víctima, lo que ocasiona un problema para el algoritmo de detección ya que no se puede diferenciar cuando existió un movimiento brusco o simplemente fue la actividad de correr.

Debido a este problema, adicionalmente al valor umbral se planteó otra condición para poder diferenciar un movimiento brusco al momento de realizar actividades similares a las de correr en las que existen varios valores de la resultante mayores a 20 m/s^2. La única diferencia entre la realización de un movimiento brusco y un movimiento repetitivo como el correr, es que después de un movimiento brusco existe un gran numero de muestras que son menores a 20 m/s^2 como se puede observar en la Figura 10, donde existen más

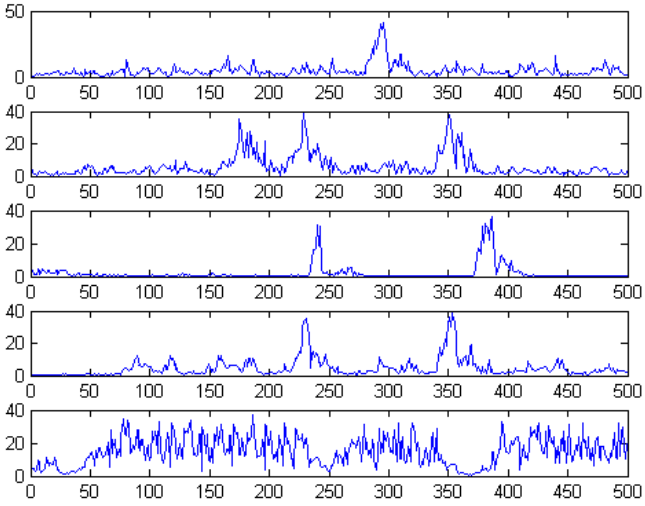


Fig. 8: Gráfica de las resultantes al realizar las actividades con movimientos bruscos.

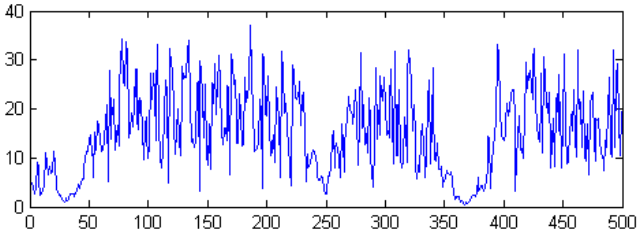


Fig. 9: Gráfica de la resultante al realizar la actividad de correr con movimientos bruscos.

de 50 valores que están por debajo de la línea roja es decir que son menores a 20 m/s^2, con esta característica particular de la señal de la aceleración resultante se pudo finalmente implementar un algoritmo que pueda distinguir un movimiento brusco de cualquier otro tipo de actividad o movimiento.

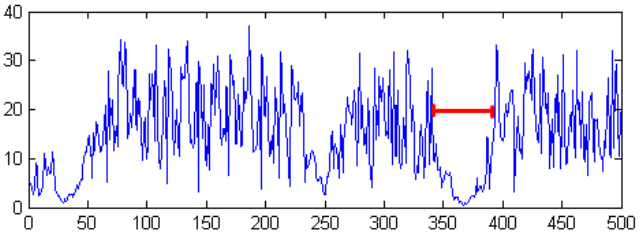


Fig. 10: Detección de un movimiento brusco al realizar la actividad de correr.

El algoritmo implementado trabaja a partir del vector que contiene los valores de las aceleraciones resultantes calculadas

para cada prueba, y su diagrama de flujo se muestra en la Figura 11.

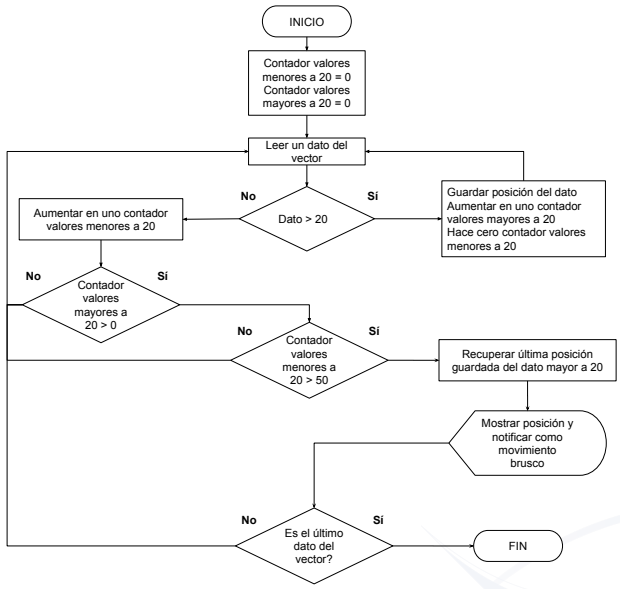


Fig. 11: Algoritmo de detección de movimientos bruscos.

B. Diseño e implementación del algoritmo de recreación

El algoritmo trabaja a partir de un conjunto de datos los cuales se resumen en la Tabla II. Todos estos datos se obtienen de los dos archivos generados por la aplicación móvil.

Datos
Angulo (Azimuth)
Altura
Componentes x, y, z del acelerómetro

Tabla II. Datos necesarios para la implementación del algoritmo de recreación.

El algoritmo realizado obtiene un vector cuyos elementos corresponden a las aceleraciones resultantes, esto con la finalidad de posteriormente comprobar si la víctima no tuvo movimiento alguno. Para lo cual se comparará con el valor de 1.7 ya que al estar el teléfono sin movimiento todos los datos de la aceleración resultante son menores a dicho valor. Luego convierte de grados a radianes un dato del vector de ángulos, verifica si un dato del vector de las aceleraciones resultantes (misma posición que el dato del vector de ángulos) es menor a 1.7, si el dato no lo es la variable modulo aumenta una unidad. Si el dato lo es el contador de valores menores a 1.7 aumenta una unidad y luego verifica si dicho contador es mayor a 20, si lo es la variable modulo no aumenta, por otra parte si el contador no es mayor a 20 entonces la variable modulo aumenta una unidad. Finalmente se obtienen las componentes x, y de la variación de ángulo y la variación de modulo, y se suma a las mismas el valor anterior de las componentes x, y, estos valores son almacenados en dos vectores.

Este proceso se lo realiza hasta finalizar todos los datos del vector de ángulos, una vez finalizados se grafica en tres dimensiones el vector de altura, el vector de la componente x y el vector de la componente y, teniendo así la recreación resultante.

C. Funcionamiento general de la aplicación

La aplicación móvil realiza la creación de varios archivos, uno por cada hora, con el objetivo de optimizar el sistema de almacenamiento descartando aquellos archivos correspondientes a horas en los que no se registró actividad motriz inusual. Por lo tanto, la aplicación de escritorio, fue diseñada e implementada de tal forma que permita el análisis de la actividad motriz de una víctima una hora a la vez. En la Figura 18 del Anexo 1 se muestra la interfaz gráfica de la aplicación de escritorio en ejecución.

En la sección **Selección de archivos**, se realiza la selección de los dos archivos que contienen la información recogida de los diferentes sensores del teléfono móvil durante una hora específica. La selección de archivos constituye el primer paso para la correcta ejecución de la aplicación y se puede realizar en cualquier momento.

En el panel **Cargar movimientos bruscos**, un botón ejecuta el mismo algoritmo de detección diseñado e implementado en esta investigación, los resultados se muestran como una lista de fechas y horas de ocurrencia correspondientes a los eventos de actividad inusual detectados en la hora de análisis. A partir de esta lista se puede realizar una navegación en el tiempo y al seleccionar un ítem de la misma, la aplicación muestra en detalle la información referente a las coordenadas geográficas del sitio del suceso (véase Figura 12).

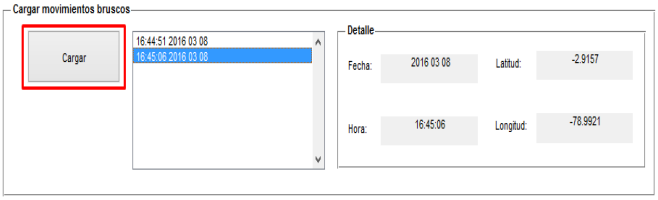


Fig. 12: Cargar movimientos bruscos.

En el siguiente panel de la interfaz gráfica, denominado **Aceleración resultante**, existen varios elementos, uno de ellos y el más grande, es un **axes** que permite la visualización de la aceleración resultante con respecto al número de muestras durante un intervalo definido de tiempo. Este intervalo es tanto para muestras anteriores así como para muestras posteriores, con centro en el número de muestra en el que ocurrió el movimiento brusco, es así que, si se seleccionó un intervalo correspondiente a 500 muestras, la aplicación graficará la aceleración resultante correspondiente a 500 muestras anteriores y posteriores a la muestra de ocurrencia. Mediante el botón **OK** se puede actualizar el número de muestras a graficarse, así

como obtener la equivalencia total en segundos del intervalo introducido. Al pulsar el botón **Graficar Todo** se ignora el intervalo introducido por el usuario y se toman todas las muestras obtenidas en los 3600 segundos correspondientes a la hora de análisis para el gráfico de la aceleración resultante. Se consideró necesaria la visualización de la aceleración resultante dentro de la interfaz de la aplicación ya que a partir de esta se puede tener una noción del tipo de actividad realizada por la víctima al momento de la detección de un movimiento brusco. En esta sección también se muestra el número total de pasos dados por la víctima, y en función a esta magnitud se calcula la cantidad total de metros recorridos, en este último computo se tomó como equivalencia que un paso sea igual 0.8 metros (véase Figura 18).

La función del botón **Simulación 3D**, ubicado en la sección lateral derecha de la interfaz (véase Figura 18), es la de mostrar dos nuevas interfaces en las cuales se grafica la trayectoria de la víctima en tres dimensiones según el intervalo de muestras y tiempo previamente elegido.

En la primera interfaz se realiza una recreación animada en la que un círculo traza la trayectoria desde el inicio hasta el final del intervalo, mediante el botón **Refrescar** se puede apreciar nuevamente la animación. Esta animación es importante ya que otorga al usuario un mayor grado de comprensión sobre los desplazamientos dados por la víctima al momento del incidente (véase Figura 13).

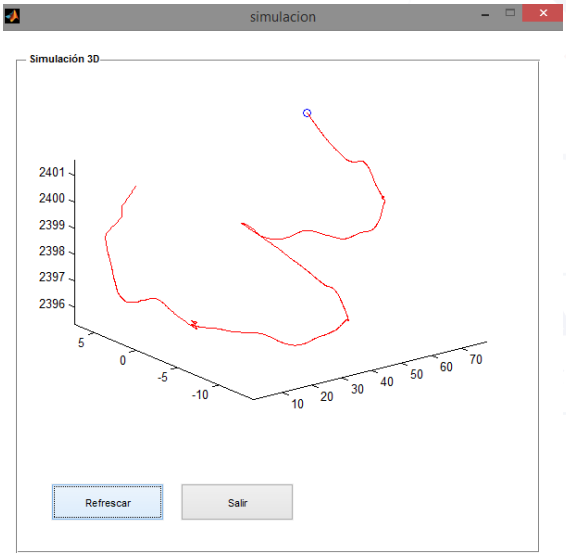


Fig. 13: Animación de la trayectoria en tres dimensiones.

En la segunda interfaz únicamente se grafica la trayectoria sin ningún tipo de animación pero se agregan herramientas que permiten la rotación, acercamiento y alejamiento de la gráfica. Mediante estas herramientas es posible apreciar la trayectoria desde varios ángulos y planos, además se señalan los puntos de ocurrencia de movimientos bruscos mediante círculos rojos (véase Figura 14).

Por último, el botón **Geolocalización** ubicado en la misma

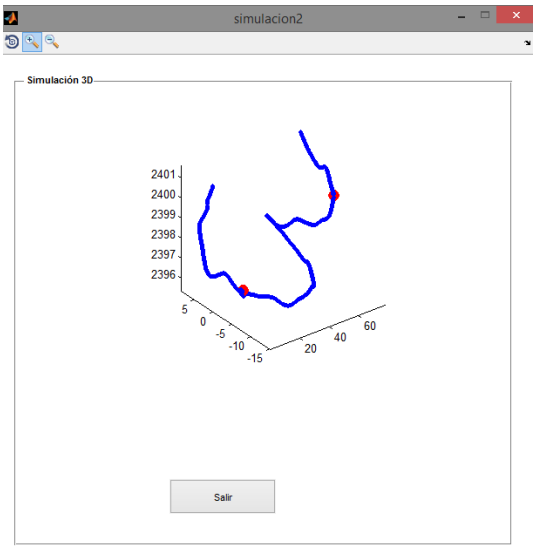


Fig. 14: Gráfico de la trayectoria en tres dimensiones.

sección que el botón **Simulación 3D** (véase Figura 18), permite ubicar en un mapa global el lugar en el que ocurrió el siniestro mediante el uso del archivo **plot_google_map.m** creado por **Zohar Bar-Yehuda** y obtenido en [2], página oficial de MATLAB para el intercambio de archivos entre la comunidad de usuarios del software. Este archivo toma como parámetros de entrada únicamente la latitud y longitud del punto en formato decimal, y presenta los resultados en una nueva interfaz como se muestra en la Figura 15.

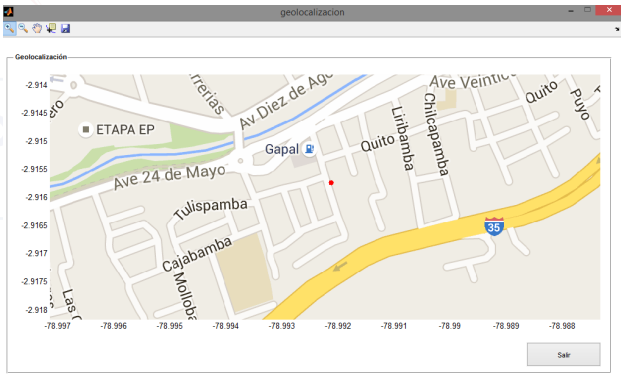


Fig. 15: Geolocalización a partir de las coordenadas del sitio del suceso.

IV. Experimentos y resultados

Para la detección de movimientos bruscos se realizaron dos conjuntos de pruebas, el primer conjunto se lo realizó con las actividades ya mencionadas anteriormente sin movimientos bruscos y el segundo conjunto se realizó con las mismas

actividades pero con movimientos bruscos.

En la Tabla III se puede observar el porcentaje de efectividad que tiene el algoritmo para las diferentes actividades realizadas sin movimientos bruscos.

Actividades realizadas	**Porcentaje de efectividad del algoritmo (%)**
Subir gradas	100
Bajar Gradas	100
De pie	100
Caminar	100
Correr	100
Promedio	**100**

Tabla III. Porcentaje de efectividad del algoritmo de detección aplicado al realizar las actividades sin movimientos bruscos.

Como se puede observar en la Tabla III, cada una de las actividad realizadas sin movimientos bruscos tienen una efectividad del 100% al aplicar el algoritmo de detección, es decir que la cantidad obtenida de movimientos bruscos es igual a la cantidad de movimientos bruscos realizados en la práctica. Entonces se puede decir que el algoritmo tiene un valor promedio del 100% de precisión cuando se aplica en actividades sin movimientos bruscos.

En la Tabla IV se puede observar el porcentaje de efectividad que tiene el algoritmo para las diferentes actividades realizadas con movimientos bruscos.

Actividades realizadas	**Porcentaje de efectividad del algoritmo (%)**
Subir gradas	100
Bajar Gradas	100
De pie	100
Caminar	100
Correr	66.67
Promedio	**93.33**

Tabla IV. Cantidad de movimientos bruscos calculados vs. real al realizar las actividades sin movimientos bruscos.

Como se puede observar en la Tabla IV, existen cuatro actividades con un porcentaje del 100% de efectividad no así para la actividad de correr con movimientos bruscos, en la cual el porcentaje de efectividad es del 66.67%, esto se debe a que en dicha actividad se producen muchos valores mayores a 20 m/s^2 en la aceleración resultante y a pesar de la segunda condición planteada en el algoritmo algunos de estos valores se detectan como movimientos bruscos aunque en realidad no lo sean. Entonces se puede afirmar que el algoritmo no tiene un valor promedio del 100% de precisión cuando se aplica en actividades con movimientos bruscos. Para las pruebas realizadas se obtuvo una precisión promedio del 93.33%. Este valor no siempre es el mismo, dependerá de los tipos de movimientos o actividades que se realicen ya que pueden existir actividades en las que al aplicarlas el algoritmo puedan reflejar movimientos bruscos aunque en la practica no existan como ya se mencionó anteriormente.

Con la finalidad de comprobar el correcto funcionamiento de la aplicación se realizaron varias pruebas de campo en diferentes lugares. A continuación se muestran dos pruebas realizadas en lugares con diferente arquitectura para poder comprobar que el algoritmo de recreación y la aplicación funcionan de manera correcta. Cabe recalcar que las pruebas se realizaron con el teléfono móvil en la mano así como también colocado en uno de los bolsillos delanteros del pantalón de la víctima, lugares en donde comúnmente se mantiene el teléfono inteligente.

En la Figura 16 se puede observar unas escaleras que tienen una forma particular la cuales pertenecen a una edificación de la Universidad de Cuenca, se denota el inicio de la trayectoria con la letra “I” y el final con la letra “F”, la recreación de la trayectoria realizada en dicho lugar se puede apreciar en la Figura 17.

Fig. 16: Gráfico del sitio de la trayectoria de la prueba 1.

V. Conclusiones

Luego de lo expuesto a lo largo de las diferentes secciones que forman parte de la presente investigación, se puede afirmar que uno de los ejes principales de la misma constituye la adquisición de datos de un teléfono inteligente. Estos dispositivos cuentan con una gran cantidad de sensores

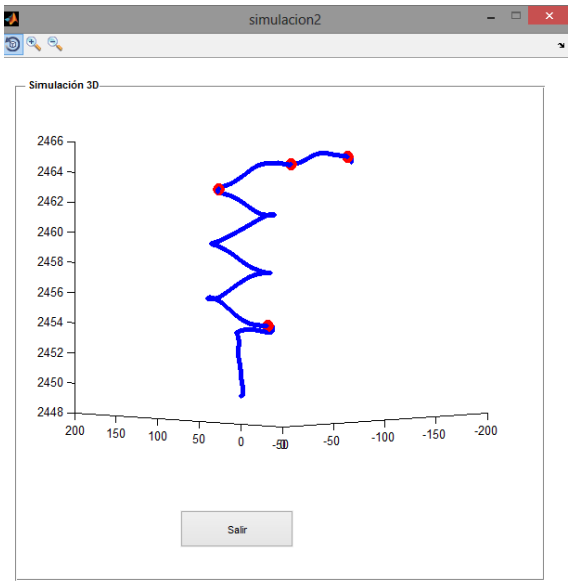


Fig. 17: Gráfico de la reconstrucción de la trayectoria de la prueba 1.

y métodos relacionados a los mismos que son capaces de proporcionar variada información, convirtiéndolos en potenciales fuentes de evidencia digital. El seleccionar adecuadamente los sensores según las necesidades y objetivos del trabajo, representa un parte crucial de la investigación, y gracias a esto fue posible desarrollar herramientas y obtener resultados de gran relevancia para el análisis digital forense.

Con el fin de detectar actividad motriz inusual o movimientos bruscos se optó por la utilización de la información proveniente del acelerómetro del teléfono inteligente, sin embargo, debido a la presencia de la gravedad de la Tierra y su influencia en las mediciones, se estableció que no solo es necesario obtener las aceleraciones registradas en los tres ejes del dispositivo sino que estas deben ser aceleraciones lineales, es decir aquellas en las que se anula por completo la gravedad. El uso de aceleraciones que no son del tipo lineal genera en el algoritmo de detección resultados erróneos ya que este, buscando lograr su objetivo de la forma más precisa posible, utiliza como principal parámetro a la aceleración resultante, cantidad que se ve afectada por la magnitud de la gravedad que se distribuye en los tres ejes del dispositivo según su posición de no anularse su efecto.

Uno de los aspectos importantes del algoritmo de detección de movimientos bruscos, es que logra cumplir su cometido sin importar el tipo de activad que haya estado realizando la víctima cuando ocurrió un incidente. Por ejemplo, se demostró que a pesar de que la víctima permanece estática, caminando, corriendo, subiendo o bajando escaleras, se logra la detección de manera exitosa. Esto se debe a que la aceleración resultante, además de resumir en una sola magnitud las tres componentes referentes a los ejes del teléfono inteligente, constituye una medida característica del movimiento de la víctima y más aún ante la ocurrencia de actividad inusual. Se intento extraer características de las tres señales de aceleraciones lineales obtenidas mediante el cálculo de otras medidas matemáticas y estadísticas con el fin de robustecer al algoritmo, pero se determinó que los resultados no eran contundentes ya que no demostraban la ocurrencia de algún movimiento inusual, justificándose así, la utilización de la aceleración resultante como único parámetro para la detección.

En cuanto al algoritmo para la recreación gráfica de la trayectoria de la víctima en tres dimensiones, se puede decir que los resultados obtenidos cuentan con un alto grado de exactitud y precisión. En primera instancia se pensaba utilizar los mismos datos de las aceleraciones lineales de los tres ejes del dispositivo para la obtención de desplazamientos mediante una doble integración, sin embargo, y luego de una minuciosa indagación sobre el tema, se decidió que este no era el camino a tomar debido al error que puede generar una integración numérica en los resultados. También se omitió el uso del GPS con el objetivo de evitar recreaciones erróneas en ambientes del tipo *indoor*. Finalmente la solución recayó nuevamente en la adquisición de datos del teléfono inteligente, esta vez se optó por la extracción de información angular referente a la orientación del dispositivo además de su altura con respecto al nivel del mar obteniéndose resultados positivos en la implementación del algoritmo con estos datos.

Se tuvo especial cuidado al momento de extraer información referente a la geolocalización de la víctima, restringiendo la adquisición de coordenadas del GPS únicamente ante la detección de eventos inusuales. Este fue un tema de importancia al momento de implementar la aplicación Android con el fin de evitar una violación a la privacidad de la víctima. También se hizo énfasis en la optimización del sistema de almacenamiento ya que toda la información recopilada de los sensores se guarda en archivos de texto y a pesar de que su tamaño individual es relativamente pequeño, luego de un uso prolongado de la aplicación, se puede generar una sobrecarga en la memoria interna del dispositivo. Dicha optimización consiste principalmente en la creación de nuevos archivos por cada hora de uso de la aplicación, de esta forma al finalizar este periodo de tiempo, la aplicación tiene la capacidad de eliminar aquellos archivos en los que no se registro ningún tipo de actividad motriz inusual por parte de la víctima.

Finalmente es necesario acotar que algunos de los datos extraídos del teléfono inteligente no son del todo exactos, por ejemplo se pudo apreciar que al correr la aplicación móvil en distintos dispositivos, en un mismo lugar, se obtenían lecturas distintas en cuanto a la altura sobre el nivel del mar. También existen ocasiones en que los datos provistos por el GPS tienen un pequeño error cuando el dispositivo se encuentra en ambientes del tipo *indoor*. Por último, se detectaron falencias en el contador de pasos

utilizado en esta investigación, una de estas es que se tarda en entregar los primeros resultados al momento de ejecutar por primera vez la aplicación y en unas pocas ocasiones no se detectó correctamente el instante en el que se da un paso.

A criterio de los investigadores, cada una de las herramientas desarrolladas en la presente investigación pudieran ser utilizadas de manera exitosa en investigaciones relacionadas al análisis digital forense. La extracción de datos a partir de los sensores de un teléfono inteligente mediante la aplicación desarrollada, cumple con el principio de fiabilidad ya que se evitó la manipulación de la información por parte del software dado que únicamente realiza procesos de obtención y almacenamiento de datos en el dispositivo. Además, la aplicación de escritorio ofrece varias herramientas que facilitan el entendimiento de los hechos ocurridos en el sitio del suceso en base a los datos obtenidos, estas herramientas permiten la visualización y animación de la trayectoria seguida por la víctima en tres dimensiones, ubicación en un mapa global de las coordenadas del sitio en el que ocurrió el siniestro y la determinación de la distancia total recorrida por la víctima. Se puede decir que la aplicación móvil y la aplicación de escritorio, utilizadas en conjunto, constituyen un recurso valedero para lograr la resolución de un caso.

REFERENCIAS:

[1] "Android Developers," 2016, Accedido 25-Febrero-2016. [En línea]. Disponible: http://developer.android.com/intl/es/guide/topics/sensors/sensors_overview.html

[2] "MathWorks File Exchange," 2016, Accedido 08-Marzo-2016. [En línea]. Disponible: http://www.mathworks.com/matlabcentral/fileexchange/27627-zoharby-plot-google-map

[3] D. Kotze y M. S. Olivier, "Patlet for digital forensics first responders," 2007.

[4] "Acpo good practice guide acpo good practice guide for digital evidence," Association of Chief Police Officers, 2012.

[5] *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*, ISO/IEC 27037, Nov. 2012.

[6] A. M. Marshall, *Digital forensics: Digital evidence in criminal investigations*. John Wiley & Sons, 2009.

[7] M. G. Kirschenbaum, R. Ovenden, G. Redwine, y R. Donahue, *Digital forensics and born-digital content in cultural heritage collections*. Council on Library and Information Resources, 2010.

[8] G. Palmer *y otros*, "A road map for digital forensic research," in *First Digital Forensic Research Workshop, Utica, New York*, 2001.

[9] H. C. Lee, T. Palmbach, y M. T. Miller, *Henry Lee's crime scene handbook*. Academic Press, 2001.

[10] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press, 2011.

[11] J. R. Kwapisz, G. M. Weiss, y S. A. Moore, "Activity recognition using cell phone accelerometers," *ACM SigKDD Explorations Newsletter*, vol. 12, num. 2, pp. 74–82, 2011.

[12] R. Feliz, E. Zalama, y J. G. García-Bermejo, "Estimación de posición de viandantes mediante sensores inerciales."

[13] D. Gafurov, E. Snekkenes, y P. Bours, "Spoof attacks on gait authentication system," *Information Forensics and Security, IEEE Transactions on*, vol. 2, num. 3, pp. 491–502, 2007.

[14] G. de Souza Faria y H. Y. Kim, "Identification of pressed keys from mechanical vibrations," *Information Forensics and Security, IEEE Transactions on*, vol. 8, num. 7, pp. 1221–1229, 2013.

[15] Y. Yuan, C. Wang, J. Zhang, J. Xu, y M. Li, "An ensemble approach for activity recognition with accelerometer in mobile-phone," in *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on*. IEEE, 2014, pp. 1469–1474.

[16] P. Siirtola y J. Röning, "Recognizing human activities user-independently on smartphones based on accelerometer data," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 1, num. 5, 2012.

[17] K. Seifert y O. Camacho, "Implementing positioning algorithms using accelerometers," *Freescale Semiconductor*, 2007.

[18] D. Coskun, O. D. Incel, y A. Ozgovde, "Phone position/placement detection using accelerometer: Impact on activity recognition," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on*. IEEE, 2015, pp. 1–6.

ANEXO 1

Fig. 18: Interfaz gráfica principal de la aplicación de escritorio.

Bibliografía

[1] M. Báez, Á. Borrego, J. Cordero, L. Cruz, M. González, F. Hernández, D. Palomero, J. R. de Llera, D. Sanz, M. Saucedo *y otros*, "Introducción a android," 1997.

[2] M. Correa Ríos, "Composición del sistema operativo móvil ios de apple y el hardware y software que lo utilizan," 2014.

[3] I. Gomez y O. Eduardo, "Arquitectura de la plataforma de desarrollo de windows phone 7," 2010.

[4] M. Liu, "A study of mobile sensing using smartphones," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[5] A. M. Marshall, *Digital forensics: Digital evidence in criminal investigations*. John Wiley & Sons, 2009.

[6] "Android Developers," 2016, Accedido 25-Febrero-2016. [En línea]. Disponible: http://developer.android.com/intl/es/reference/android/hardware/SensorEvent.html

[7] M. de Justicia Derechos Humanos y Cultos, "Código orgánico integral penal," 2014. [En línea]. Disponible: http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

[8] D. Kotze y M. S. Olivier, "Patlet for digital forensics first responders," 2007.

[9] Forensics Wiki, "Famous Cases Involving Digital Forensics," 2013, Accedido 10-Febrero-2016. [En línea]. Disponible: http://forensicswiki.org/wiki/Famous_Cases_Involving_Digital_Forensics

[10] V. S. Venkitachalam, V. Namboodiri, S. Joseph, E. Dee, y C. A. Burdsal, "What, why, and how: Surveying what consumers want in new mobile phones." *Consumer Electronics Magazine, IEEE*, vol. 4, num. 2, pp. 54–59, 2015.

[11] statista:The Statistics Portal, "Smartphone user penetration as percentage of total global population from 2011 to 2018*," 2015, Accedido 10-Febrero-2016. [En línea]. Disponible: http://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/

[12] M. G. Kirschenbaum, R. Ovenden, G. Redwine, y R. Donahue, *Digital forensics and born-digital content in cultural heritage collections.* Council on Library and Information Resources, 2010.

[13] G. Palmer *y otros*, "A road map for digital forensic research," in *First Digital Forensic Research Workshop, Utica, New York*, 2001.

[14] A. M. Marshall, *Digital forensics: Digital evidence in criminal investigations.* John Wiley & Sons, 2009.

[15] H. C. Lee, T. Palmbach, y M. T. Miller, *Henry Lee's crime scene handbook.* Academic Press, 2001.

[16] *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*, ISO/IEC 27037, Nov. 2012.

[17] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet.* Academic press, 2011.

[18] E. Martínez, "La evolución de la telefonía móvil," *articulo publicado en la revista RED*, 2001.

[19] M. Gorricho Moreno y J. L. Gorricho Moreno, *Comunicaciones móviles.* Edicions UPC, 2002.

[20] M. R. Bhalla y A. V. Bhalla, "Generations of mobile wireless technology: A survey," *International Journal of Computer Applications*, vol. 5, num. 4, 2010.

[21] J. Neira, "End-of-life management of cell phones in the united states," Ph.D. dissertation, UNIVERSITY OF CALIFORNIA Santa Barbara, 2006.

[22] C. Glanzer, J. Kuehl, y R. Vettern, "Smartphone user and application safety," Ph.D. dissertation, North Dakota State University, 2011.

[23] O. Okediran, O. Arulogun, y R. Ganiyu, "Mobile operating systems and application development platforms: A survey," *Journal of Advancement in Engineering and Technology*, vol. 1, 2014.

[24] J. C. CHEANG WONG, "Ley de moore, nanotecnología y nanociencias: Síntesis y modificación de nanopartículas mediante la implantación de iones," *Revista Digital Universitaria*, 2005.

[25] U. Shala y A. Rodriguez, "Indoor positioning using sensor-fusion in android devices," 2011.

[26] A. Pande, Y. Zeng, A. K. Das, P. Mohapatra, S. Miyamoto, E. Seto, E. K. Henricson, y J. J. Han, "Energy expenditure estimation with smartphone body sensors," in *Proceedings of the 8th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 8–14.

[27] "Acpo good practice guide acpo good practice guide for digital evidence," Association of Chief Police Officers, 2012.

[28] J. R. Kwapisz, G. M. Weiss, y S. A. Moore, "Activity recognition using cell phone accelerometers," *ACM SigKDD Explorations Newsletter*, vol. 12, num. 2, pp. 74–82, 2011.

[29] Y. Yuan, C. Wang, J. Zhang, J. Xu, y M. Li, "An ensemble approach for activity recognition with accelerometer in mobile-phone," in *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on*. IEEE, 2014, pp. 1469–1474.

[30] P. Siirtola y J. Röning, "Recognizing human activities user-independently on smartphones based on accelerometer data," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 1, num. 5, 2012.

[31] R. Feliz, E. Zalama, y J. G. García-Bermejo, "Estimación de posición de viandantes mediante sensores inerciales."

[32] D. Gafurov, E. Snekkenes, y P. Bours, "Spoof attacks on gait authentication system," *Information Forensics and Security, IEEE Transactions on*, vol. 2, num. 3, pp. 491–502, 2007.

[33] G. de Souza Faria y H. Y. Kim, "Identification of pressed keys from mechanical vibrations," *Information Forensics and Security, IEEE Transactions on*, vol. 8, num. 7, pp. 1221–1229, 2013.

[34] D. Coskun, O. D. Incel, y A. Ozgovde, "Phone position/placement detection using accelerometer: Impact on activity recognition," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on*. IEEE, 2015, pp. 1–6.

[35] K. Seifert y O. Camacho, "Implementing positioning algorithms using accelerometers," *Freescale Semiconductor*, 2007.

[36] "Android Developers," 2016, Accedido 25-Febrero-2016. [En línea]. Disponible: http://developer.android.com/intl/es/reference/android/hardware/SensorManager.html

[37] "Android Developers," 2016, Accedido 25-Febrero-2016. [En línea]. Disponible: http://developer.android.com/intl/es/guide/topics/sensors/sensors_overview.html

[38] "Android Developers," 2016, Accedido 25-Febrero-2016. [En línea]. Disponible: http://developer.android.com/intl/es/guide/topics/sensors/sensors_motion.html#sensors-motion-accel

[39] "MathWorks File Exchange," 2016, Accedido 08-Marzo-2016. [En línea]. Disponible: http://www.mathworks.com/matlabcentral/fileexchange/27627-zoharby-plot-google-map